La protection des lanceurs d'alerte (Whistleblowers) à l'heure d'Internet

Lachapelle, Amélie

Published in:
L'Europe des droits de l'homme à l'heure d'Internet

Publication date:
2019

Document Version
le PDF de l'éditeur

CHAPITRE 6. LA PROTECTION DES LANCEURS D'ALERTE (WHISTLEBLOWERS) À L'HEURE D'INTERNET*

Amélie LACHAPELLE[1]
Doctorante Aspirante F.R.S.-FNRS à l'UNamur
Co-directrice de l'unité Libertés, Information et Société du CRIDS/NADI (UNamur)
Membre associée du CRECO (UCLouvain)

I. Introduction

1. La dénonciation se pratique depuis la nuit des temps, ou presque. L'approche qu'on en a aujourd'hui, propre au débat suscité par les lanceurs d'alerte, est toutefois résolument novatrice. La popularité de cette catégorie singulière de dénonciateurs résiderait, selon Jean-Paul Brodeur, dans l'inversion qu'elle initie de la relation d'asymétrie propre à la délation[2]. Tandis que les délateurs livreraient au plus fort les plus faibles, les lanceurs d'alerte feraient exactement l'inverse, prenant le parti des plus faibles pour se livrer à un combat digne de celui de David contre Goliath.

L'actualité des dernières années, et des dernières semaines, nous a montré à suffisance le rôle cardinal joué par les lanceurs d'alerte dans la révélation d'informations d'intérêt général. Que l'on pense à l'affaire « *Snowden* », à celle des « *Panama Papers* » ou encore à celle toute récente des « *Cambridge Analytica Files* », tous ces scandales ont pu éclater au grand jour grâce à l'intervention de ce que l'on appelle désormais des « lanceurs d'alerte ». Le puissant vecteur de communication que représente Internet a, du reste, joué un rôle majeur, tant dans la

* Propos arrêtés à la date du 28 avril 2018.

1 L'auteure remercie Quentin Van Enis, chargé de cours invité à la Faculté de droit de l'UNamur, chercheur au CRIDS/NADI et avocat au barreau de Bruxelles, pour sa relecture attentive du présent texte, ses remarques avisées et les discussions qui s'en sont suivies.

2 J.-P. BRODEUR, « Introduction : la délation organisée », in *Citoyens et délateurs. La délation peut-elle être civique ?* (J.-P. BRODEUR et F. JOBARD dir.), Paris, Autrement, 2005, p. 210.

transmission d'informations confidentielles, que dans leur traitement et enfin dans leur diffusion mondiale.

La nécessité de protéger, dans une société démocratique, les lanceurs d'alerte n'est plus à démontrer : de bonnes sources d'informations sont, de fait, indispensables en vue de permettre au public de se forger des opinions éclairées sur les questions d'intérêt général[3]. Elles sont, par ailleurs, essentielles aux organes de gouvernance, institués au sein des entreprises et administrations, et aux autorités publiques en vue de détecter, poursuivre et juger les infractions aux normes en vigueur.

Au-delà du rôle traditionnel d'auxiliaire de justice que leur confie l'institution américaine du *whistleblowing*[4] dont ils tirent leur origine, les lanceurs d'alerte (« *whistleblowers* ») exercent aussi de nos jours une fonction de vigie citoyenne dans la défense des droits de l'homme.

Dans un tel contexte, un projet de texte devait finir par éclore au niveau européen. C'est chose faite depuis le 23 avril dernier. La Commission européenne a présenté une proposition de directive visant à garantir un niveau élevé de protection des lanceurs d'alerte qui signalent des violations potentielles ou avérées du droit de l'UE[5].

2. Le présent chapitre se compose de trois sections. Après avoir exposé les éléments-clés d'une définition juridique du « lancement d'alerte » en Europe (II), nous reviendrons sur les principaux textes européens en la matière, en veillant à mettre en évidence la dualité qui traverse le concept de lancement d'alerte en droit européen (III). Enfin, et c'est là le cœur du chapitre (IV), nous ferons le point sur la protection concrète que confèrent au lanceur d'alerte le droit à la liberté d'expression (IV, A) et le droit à la vie privée et à la protection des données (IV, B). Au croisement de ces deux droits fondamentaux se niche un droit d'une importance capitale à l'ère tant des lanceurs d'alerte que d'Internet : le droit au chiffrement et à l'anonymat (IV, C).

3 En ce sens, voy. not. rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression David Kaye sur la protection des sources d'information et des lanceurs d'alerte, A/70/361, 8 septembre 2015, pp. 9 et 15.

4 Littéralement : « fait de souffler dans le sifflet ».

5 Proposition de directive du 23 avril 2018 relative à la protection des personnes signalant des violations du droit de l'Union (COM(2018) 218 final) (ci-après « proposition de directive du 23 avril 2018 »).

II. La notion juridique de « lancement d'alerte » à l'heure d'Internet

3. Forme singulière de dénonciation, le lancement d'alerte ne jouit actuellement d'aucune définition univoque en droit européen[6]. Un consensus se dégage néanmoins sur ses éléments constitutifs, au nombre de quatre : le lanceur d'alerte (A), l'acte de signalement (B), la partie auprès de qui le signalement est effectué, soit le destinataire (C) et l'organisation concernée, directement ou indirectement, par le lancement d'alerte (D).

A. – *Le lanceur d'alerte*

4. En Europe, le statut de lanceur d'alerte ne semble pouvoir être reconnu qu'à une personne qui signale des informations concernant une menace ou un préjudice pour l'intérêt général dans le contexte de sa relation de travail, qu'elle soit dans le secteur public ou dans le secteur privé[7].

Une protection légale spécifique s'impose ici pour trois motifs. Tout d'abord, le travailleur jouit d'un accès privilégié aux informations de l'organisation pour laquelle il travaille[8]. Partant, il « est seul à savoir – ou fait partie d'un petit groupe dont les membres sont seuls à savoir – ce qui se passe sur son lieu de travail et est donc le mieux placé pour agir dans l'intérêt général en avertissant son employeur ou l'opinion publique »[9]. Ensuite, il se trouve dans une évidente situation de vulnérabilité économique vis-à-vis de son employeur, duquel dépend *de facto* son emploi[10]. Enfin, ce lien de subordination va de pair avec un devoir de loyauté, de réserve et de discrétion à l'égard de l'employeur[11]. Amené à « opposer

6 Voy. not. *Commission Staff Working Document*, *Impact Assessment accompanying the document* « Proposal for a Directive of the European Parliament and of the Council on the protection of persons reporting on breaches of Union law » (SWD(2018) 116 final), p. 6.

7 Recommandation CM/Rec (2014) 7 sur la protection des lanceurs d'alerte, adoptée par le Comité des ministres du Conseil de l'Europe le 30 avril 2014, annexe, définitions, a). Voy. aussi proposition de directive du 23 avril 2018, art. 2 et considérant n° 25 ; le document de travail publié par la Commission européenne en vue de la consultation publique organisée du 3 mars au 29 mai 2017 à propos de la protection des lanceurs d'alerte (p. 2) : G29, avis n° 1/2006 du 1er février 2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière (ci-après « avis n° 1/2006 »), WP 117, p. 6.

8 Proposition de directive du 23 avril 2018, considérant n° 25.

9 Voy. not. Cour eur. D.H. (5e sect.), 21 juillet 2011, req. n° 28274/08, *Heinisch c. Allemagne*, § 63.

10 Proposition de directive du 23 avril 2018, considérant n° 24.

11 Voy. not. Cour eur. D.H. (Gde ch.), 27 juin 2017, req. n° 17224/11, *Medzlis Islamske Zajednice Brcko et autres c. Bosnie-Herzégovine*, § 80.

une loyauté à une autre » – celle de son organisation, d'une part, et celle de la société dans laquelle il évolue, d'autre part – le travailleur doit faire face à un inévitable « conflit de loyautés »[12].

5. L'appréciation du champ d'application personnel se veut large. Ainsi, si en l'état actuel de la jurisprudence de la Cour européenne des droits de l'homme, le statut protecteur de lanceur d'alerte n'a été accordé qu'à un fonctionnaire ou un employé, il semble établi que la notion de « travailleur » doit également inclure les travailleurs temporaires et à temps partiel, les stagiaires, les bénévoles ainsi que les anciens et futurs employés[13].

Au delà de la relation stricte de travail, la proposition de directive déposée par la Commission européenne le 23 avril dernier entend étendre la notion à d'autres catégories de personnes physiques ou morales qui, sans être « travailleurs » au sens de l'article 45 TFUE, peuvent jouer un rôle clé dans la révélation de manquements au droit de l'Union et peuvent se trouver, eu égard à leur relation professionnelle, dans une situation de vulnérabilité économique[14]. On pense, par exemple, aux clients, fournisseurs et autres cocontractants, actionnaires et autres tiers en rapport avec l'employeur[15], soit à l'ensemble des personnes gravitant autour de l'organisation sous le contrôle duquel les irrégularités sont susceptibles d'être commises[16].

12 Voy. not. Q. VAN ENIS, « Une solide protection des sources journalistiques et des lanceurs d'alerte : une impérieuse nécessité à l'ère dite de la "post-vérité" ? », in *Le secret*, coll. Recyclage en droit, Limal, Anthemis, 2017, p. 129, n° 41 ; C. ALFORD, *Whistleblowers : Broken Lives and Organizational Power*, Ithaca, Cornell University Press, 2002, p. 78 ; S. SCHEHR, « L'alerte comme forme de déviance : les lanceurs d'alerte entre dénonciation et trahison », *Déviance et Société*, vol. 32, n° 2, 2008, p. 157 ; M. DUPISSON, *Le droit d'alerter. Étude sur la protection de l'intégrité physique des personnes*, thèse de doctorat en droit privé et sciences criminelles, 20 novembre 2013, p. 140 ; M. P. MICELI, S. DREYFUS et J. P. NEAR, « Outsider "whistleblowers" : Conceptualizing and Distinguishing "Bell-Ringing" Behavior », in *International Handbook on Whistleblowing Research* (D. LEWIS *et al.* éd.), Cheltenham, Elgar, 2014, pp. 71-94 ; J.-Ph. FOEGLE, « Les lanceurs d'alerte. Étude comparée France – États-Unis », *La Revue des droits de l'homme*, n° 2014/6, p. 18 (mis en ligne le 29 novembre 2014, www.revdh.revues.org, consulté le 14 août 2017).

13 Recommandation CM (2014) 7, annexe, section II, principes 3 et 4 et exposé des motifs, § 45 ; proposition de directive du 23 avril 2018 relative à la protection des personnes signalant des violations du droit de l'Union (COM(2018) 218 final), art. 2 et 3 (10) et considérants n^{os} 25 et 28. Voy. aussi Transparency International, *International Principles for Whistleblower Legislation : Best Practices for Laws to Protect Whistleblowers and Support Whistleblowing in the Public Interest*, 2013, p. 4, pt 4) ; Groupe des Verts/ALE du Parlement européen, Whistleblower protection in the public and private sector in the European Union. Draft directive, 23 avril 2016, art. 3, c).

14 Proposition de directive du 23 avril 2018, art. 3 (9) et considérant n° 27.

15 Recommandation CM (2014) 7, exposé des motifs, pt 45 et proposition de directive du 23 avril 2018, art. 2.

16 En ce sens, voy. not. le rapport du Parlement européen du 10 octobre 2017 sur les mesures légitimes visant à protéger les lanceurs d'alerte qui divulguent, au nom de l'intérêt public, des informations confidentielles d'entreprises et d'organismes publics (2016/2224(INI)), § 14. Notons que des auteurs américains ont forgé, à côté du concept de « *whistle-blower* », le concept de « *bell-ringing* » pour désigner précisément l'alerte lancée par des personnes externes à l'organisation (« *outsiders* »), tels que des clients ou des consommateurs (M. P. MICELI, S. DREYFUS et J. P. NEAR, « Outsider "whistleblowers" : Conceptualizing and Distinguishing "Bell-Ringing" Behavior », *op. cit.*, pp. 71-94).

Dans le même sens, le rapport précité sur la promotion et la protection du droit à la liberté d'opinion et d'expression déconseille de limiter le statut de lanceur d'alerte au travailleur dès lors qu'une personne peut avoir connaissance d'informations d'intérêt public en dehors de sa relation de travail[17]. De même, la Convention des Nations unies contre la corruption[18], qui représente, en droit international, le principal texte de protection des lanceurs d'alerte, ne se limite pas au contexte de la relation de travail.

B. – *Le signalement*

6. Le signalement doit porter sur des informations concernant une menace ou un préjudice pour l'intérêt général et découvertes dans le contexte d'une relation de travail[19]. Que la menace soit potentielle n'a pas d'importance du moment qu'elle est susceptible de se réaliser[20]. Il peut s'agir d'actions ou d'omissions ou de toute révélation d'informations sur de tels faits[21]. En l'état actuel de sa jurisprudence, la Cour européenne des droits de l'homme a déjà eu l'occasion de se prononcer sur des conduites ou actes illicites[22], des agissements irréguliers ou discutables d'autorités publiques[23], des dysfonctionnements internes[24] et des comportements ou pratiques que le lanceur d'alerte estimait contestables[25].

7. Le lancement d'alerte a encore ceci de particulier qu'il porte sur des informations jugées confidentielles ou secrètes par l'organisation concernée. Cela signifie, aux yeux de la Cour de Strasbourg, que les informations ne sont pas facilement ou publiquement accessibles[26].

17 Rapport préc., A/70/361, pp. 15 et 16.

18 Convention des Nations unies contre la corruption (*United Nations Convention Against Corruption* – UNCAC), adoptée par l'Assemblée générale par la résolution n° 58/4 du 31 octobre 2003 et en vigueur depuis le 14 décembre 2005.

19 Recommandation CM (2014) 7, annexe, définitions, a) ; proposition de directive précitée du 23 avril 2018, considérant n° 1 ; Cour eur. D.H. (Gde ch.), 12 février 2008, req. n° 14277/04, *Guja c. Moldavie*, § 72. Voy. aussi Cour eur. D.H., *Heinisch*, préc., § 93 ; Cour eur. D.H. (2e sect.), 19 janvier 2016, req. n° 49085/07, *Görmüs et autres c. Turquie*, § 76.

20 Proposition de directive du 23 avril 2018, considérant n° 30 et art. 3(1).

21 Recommandation CM (2014) 7, annexe, définitions, b), et proposition de directive du 23 avril 2018, art. 3(2).

22 Cour eur. D.H., *Guja*, préc., § 97. Voy. aussi Cour eur. D.H., *Heinisch*, préc., §§ 43 et 93 ; Cour eur. D.H (3e sect.), 8 janvier 2013, req. n° 40238/02, *Bucur et Toma c. Roumanie*, § 120.

23 Cour eur. D.H., *Görmüs*, préc., § 74.

24 G29, avis n° 1/2006, p. 2.

25 Cour eur. D.H., *Görmüs*, préc., § 76.

26 Voy. Cour eur. D.H., *Guja*, préc., § 72 ; Cour eur. D.H. (5e sect.), 30 septembre 2010, req. n° 28369/07, *Balenović c. Croatia* (déc.) ; *Medzlis*, § 80. En ce sens, voy. not. V. JUNOD, « La liberté d'expression du whistleblower. Cour européenne des droits de l'homme (Grande chambre), *Guja c. Moldova*, 12 février 2008 », *Rev. trim. D.H.*, 2009, vol. 77, p. 245.

Ceci explique que le *whistleblowing* soit traditionnellement limité aux travailleurs dans la mesure où ce sont eux qui disposent, par hypothèse, d'un accès privilégié à l'information d'une entreprise ou d'une institution publique[27], ce que la récente proposition de directive européenne ne manque pas de souligner[28].

8. Quoique les États membres soient libres de déterminer, comme ils l'entendent, ce que recouvre la notion d'« intérêt général », les instances européennes ont émis quelques orientations sur le sujet. Le Comité des ministres du Conseil de l'Europe a notamment déclaré qu'un tel intérêt devait, « pour le moins, inclure les violations de la loi et des droits de l'homme, ainsi que les risques pour la santé et la sécurité publiques, et pour l'environnement »[29]. De son côté, la Commission européenne a choisi, dans le cadre de sa proposition de directive du 23 avril dernier, de lister une série de domaines spécifiques pour lesquels le recours aux lanceurs d'alerte s'avère nécessaire[30]. On y retrouve notamment la protection de l'environnement, la santé publique, la protection de la vie privée et des données personnelles.

En l'occurrence, les pratiques de surveillance massive menées par les gouvernements américain et britannique et dénoncées par l'ex-employé de la CIA et de la NSA, Edward Snowden, constituent une violation des droits de l'homme, en particulier du droit à la vie privée et à la protection des données et de la liberté d'expression[31]. Parmi ces pratiques, mentionnons le programme PRISM qui aurait permis au FBI et à la NSA de surveiller les internautes de la planète entière grâce à la probable collaboration des géants d'Internet tels que Google, Microsoft, Yahoo, Facebook, Skype et Apple[32].

Les États-Unis n'ont toutefois pas reconnu à Edward Snowden le statut de lanceur d'alerte. Que du contraire, ces derniers ont lancé un mandat d'arrêt à son encontre, du chef d'espionnage au sens de l'« *Espionage Act* » de 1917. En réaction, l'Assemblée parlementaire du Conseil de

27 Voy. not. P. B. JUBB, « *Whistleblowing* : A Restrictive Definition and Interpretation », *Journal of Business Ethics*, 1999, n° 21, p. 86.

28 Proposition de directive du 23 avril, mémorandum explicatif, p. 10.

29 Recommandation CM/Rec (2014) 7, annexe, section I, principe 2.

30 Proposition de directive du 23 avril 2018, art. 1, a), et annexe, partie I et II.

31 Sur cette affaire et les questions suscitées eu égard à la liberté d'expression, voy. not. F. DUBUISSON, « Société de l'information, médias et liberté d'expression », *J.E.D.H.*, 2014/3, pp. 359-363.

32 G. GREENWALD et E. MACASKILL, « NSA Prism program taps in to user data of Apple, Google and others », 7 juin 2013, *The Gardian*, https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (consulté le 1er mars 2018) ; S. ACKERMAN, « US tech giants knew of NSA data collection, agency's top lawyer insists », 19 mars 2014, *The Guardian*, https://www.theguardian.com/world/2014/mar/19/us-tech-giants-knew-nsa-data-collection-rajesh-de (consulté le 28 février 2018).

l'Europe a alors sollicité l'extension de la protection des lanceurs d'alerte aux personnes travaillant pour le compte des services de sécurité nationale ou de renseignement, sans porter atteinte aux droits de l'homme d'autrui[33].

C'est que le domaine de la sécurité nationale et du renseignement est, en réalité, très sensible[34]. Celui-ci est soumis à un cadre spécifique plus strict qui s'inspire des « Principes globaux sur la sécurité nationale et le droit à l'information », dits « Principes de Tshwane », qui ont été élaborés sous l'égide de l'*Open Society Justice Initiative*[35]. Avalisés par l'Assemblée parlementaire du Conseil de l'Europe[36], ces principes visent à fournir des orientations aux législateurs nationaux en vue de garantir un équilibre entre l'accès du public à l'information gouvernementale et la protection de la population contre les menaces qui pèsent sur la sécurité nationale, qui relèvent tous deux de l'intérêt public.

9. Une question importante reste en suspens : le lancement d'alerte peut-il porter sur des activités préjudiciables sans être illégales, voire sur des pratiques jugées immorales ? La question n'est actuellement pas tranchée. Le Comité des ministres du Conseil de l'Europe ne paraît pas opposé en ce qu'il précise, dans sa recommandation (2014) 7, que l'alerte peut également concerner, à côté de la violation de la loi, « un préjudice pour les usagers d'un service, le grand public ou l'organisation elle-même »[37]. De son côté, la Cour de Strasbourg a accueilli, dans l'affaire *Görmüs*, le signalement d'« agissements irréguliers ou discutables d'autorités publiques »[38]. Dans l'affaire *Bathellier*, elle a toutefois témoigné d'une attention certaine à la divergence de points de vue dont souffraient les allégations du requérant pour écarter l'application de sa jurisprudence *Guja*[39]. Sans doute la formulation par le requérant d'une opinion, plus que d'une constatation, a-t-elle, à cet égard, été

33 Résolution 2060(2015)1, « Améliorer la protection des donneurs d'alerte », discussion par l'Assemblée du Conseil de l'Europe le 23 juin 2015, 21e séance, § 8.

34 M. Bardin, « Les "lanceurs d'alerte" à l'ère du numérique : un progrès pour la démocratie ? », in *Protection des données personnelles et Sécurité nationale. Quelles garanties juridiques dans l'utilisation du numérique ?* (O. de David Beauregard-Berthier et A. Taleb-Karlsson coord.), Bruxelles, Bruylant, 2017, pp. 249-274. Sur la portée de la liberté d'expression dans le domaine du renseignement, voy. aussi Cour eur. D.H. (Gde ch.), 10 décembre 2007, req. n° 69698/01, *Stoll c. Suisse*. Voy. aussi résolution 1551(2007) de l'Assemblée parlementaire du Conseil de l'Europe sur l'équité des procédures judiciaires dans les affaires d'espionnage ou de divulgation de secrets d'État.

35 Recommandation CM/Rec (2014) 7, annexe, section II, principe 5 et exposé des motifs, §§ 46 et 47. Voy. aussi rapport préc., A/70/361, 8 septembre 2015, pp. 21 et 22, §§ 43 et 44.

36 Résolution 1954 (2013) intitulée « La sécurité nationale et l'accès à l'information », 2 octobre 2013.

37 Recommandation CM/Rec 2014 (7), exposé des motifs, § 2.

38 Cour eur. D.H., *Görmüs*, préc., § 74.

39 Cour eur. D.H. (5e sect.), 12 octobre 2010, req. n° 49001/07, *Bathellier c. France* (déc.).

déterminante[40], mais il nous semble que l'absence d'illégalité formelle a également pesé dans la balance.

Toujours est-il que, dans l'affaire *LuxLeaks*, la Cour d'appel du Grand-Duché de Luxembourg a soutenu, à la lumière de la jurisprudence strasbourgeoise, que l'illicéité du comportement divulgué ne conditionnait pas la mise en œuvre du statut protecteur de lanceur d'alerte[41]. Partant, la Cour a admis que la dénonciation de la pratique de l'optimisation fiscale par des entreprises transnationales[42] relevait de l'intérêt général, de par le débat public suscité sur l'imposition des sociétés, sur la transparence fiscale, la pratique des rescrits fiscaux et sur la justice fiscale en général.

Par sa proposition de directive du 23 avril dernier, la Commission européenne se dirige vers une même direction dès lors qu'elle précise que doivent être protégés, non seulement le signalement d'activités illégales, mais aussi celui d'abus de droit, à savoir des « actes ou omissions relevant du champ d'application du droit de l'Union qui ne se présentent pas en tant que tels comme illégaux mais qui nuisent aux objectifs ou aux finalités poursuivies par les règles applicables »[43].

C. – *Le destinataire du signalement : interne – externe – public*

10. Au sein du lancement d'alerte, on distingue communément trois types de signalement : le signalement interne, le signalement externe et la révélation publique[44]. Le signalement interne a lieu au sein d'une

40 Voy. Q. VAN ENIS, « Une solide protection des sources journalistiques et des lanceurs d'alerte : une impérieuse nécessité à l'ère dite de la "post-vérité" ? », *op. cit.*, p. 136, pt 59.

41 Cour d'appel du Grand-Duché de Luxembourg (10e ch.), 15 mars 2017, arrêt dans le cadre de l'affaire dite *LuxLeaks*, disponible sur le site internet www.justice.public.lu (consulté le 23 mars 2017).

42 À ce sujet, une distinction capitale doit être opérée entre la fraude fiscale et l'évasion fiscale, seule la fraude fiscale étant en règle illicite. Ceci étant, certaines pratiques d'évitement licite de l'impôt sont sanctionnées par des dispositions dites « anti-abus ». Voy. not. M. BOURGEOIS et A. NOLLET, « La réécriture de la mesure "générale anti-abus" applicable en matière d'impôts sur les revenus, de droits d'enregistrement et de droits de succession », *J.T.*, 2012, n° 6483, pp. 493-504 ; M. BOURGEOIS et A. LACHAPELLE, « Multinationales : la lutte contre l'évasion fiscale en Europe », *J.D.E.*, 2016/8, n° 232, pp. 302 et 303.

43 Proposition de directive du 23 avril 2018, art. 3(3) et considérant n° 29.

44 Voy., entre autres, ch. II et III de la proposition de directive du 23 avril 2018 ; recommandation CM/Rec (2014) 7, annexe, section IV, principe 14 ; résolution du Parlement européen du 24 octobre 2017 sur les mesures légitimes visant à protéger les lanceurs d'alerte qui divulguent, au nom de l'intérêt public, des informations confidentielles d'entreprises et d'organismes publics, 2016/2224(INI), considérant F ; Groupe des Verts/ALE du Parlement européen, Whistleblower protection in the public and private sector in the European Union. Draft directive, préc., art. 6-8 ; Office des Nations unies contre la drogue et le crime (UNODC), *Resource Guide on Good Practices in the Protection of Reporting Persons*, New York, United Nations, 2015, pp. 29-45 ; rapport A/70/361, préc., pp. 18 et 19 ; OECD, *Committing to Effective Whistleblower Protection*, Paris, OECD Publishing, 2016, p. 53. Voy. aussi la jurisprudence de la Cour européenne des droits de l'homme (Cour eur. D.H., *Guja* ; *Bathellier* (déc.) ; *Heinisch* ; *Bucur* ; *Görmüs*). Du côté de la doctrine, voy. not. T. DEVINE et T. F. MAASSARANI, *The Corporate Whistleblower's Survival Guide : a Handbook for Committing the Truth*, publié avec l'association Government Accountability Project, San

organisation ou d'une entreprise ; le signalement externe intervient auprès d'organes réglementaires publics, d'autorités de répression ou d'organes de contrôle ; la révélation publique d'informations peut se faire, quant à elle, auprès d'un journaliste, d'une organisation non gouvernementale, d'un parlementaire ou directement via une page Web ou une plateforme en ligne[45].

Indépendamment du type de signalement, on mentionnera que le lanceur d'alerte peut décider de prendre conseil auprès de son syndicat ou d'un avocat par exemple. Ce faisant, il y a fort à parier que des communications électroniques seront échangées. La proposition de directive du 23 avril dernier énonce par ailleurs qu'un conseil, un syndicat ou un fournisseur de plateforme pourrait réceptionner des signalements pour le compte d'une organisation[46].

11. Dans le cadre du présent chapitre, on insistera sur le fait que le dépôt d'une dénonciation passe aujourd'hui, presque nécessairement, par le truchement d'une plateforme ou d'une interface Web dont les données sont stockées sur un réseau informatique sécurisé[47]. On peut distinguer différents cas de figure, selon que le destinataire est capable ou non de remédier lui-même au problème dénoncé :

1) L'interface a été créée en vue de permettre le signalement en interne d'irrégularités concernant l'entreprise ou l'administration ;
2) L'interface a été créée par des autorités publiques en vue de faciliter la prise de connaissance de pratiques illégales. Tel est le cas, par exemple, du système en ligne de notification des fraudes établi par l'Office européen de lutte antifraude (voy. *infra*, n° 66) ;
3) L'interface a été créée par un groupe parlementaire, un organisme de médias ou une société privée du secteur des TIC en vue de faciliter la prise de connaissance de faits d'intérêt général dans un cadre légal lacunaire. On pense, par exemple, à la plateforme *EuLeaks*, lancée par les parlementaires européens du groupe Verts/ALE[48], au site www.source.eu, le site d'envoi anonyme de documents vers les

Fransisco, Berrett-Koehler Publishers, ch. 4 ; R. Moberly, « 12. "To Persons or Organizations that May Be Able to Effect Action": Whistleblowing Recipients », in *International Handbook on Whistleblowing Research* (D. Lewis *et al.* éd.), Cheltenham, Elgar, 2014, pp. 273-297.

45 Recommandation CM/Rec (2014) 7, annexe, section IV, principe 14. Voy. aussi la proposition de directive du 23 avril 2018, art. 3(6), (7) et (8) et considérant n° 32.

46 Proposition de directive du 23 avril 2018, considérant n° 43.

47 Notons que la proposition de directive du 23 avril 2018 précise que le signalement, qu'il soit interne ou externe, doit pouvoir se faire via un signalement électronique (art. 5.2, a), et 7.2, a)). Elle n'évoque cependant pas la problématique du recours à Internet dans la procédure de signalement, sauf à son considérant n° 42.

48 Disponible à l'adresse www.greens-efa.eu/ (consulté le 10 juin 2017).

médias[49] ou encore à la plateforme *GlobaLeaks*, qui tend à permettre un lancement d'alerte anonyme et sûr par le biais de technologies innovantes (voy. *infra*, n° 54).

Dans les deux premières hypothèses, le signalement a pour objectif de prévenir, mettre fin et/ou de sanctionner une situation irrégulière ou illégale. Dans la troisième hypothèse, le signalement sert l'objectif de transparence et de responsabilité démocratique. Rien n'empêche cependant les autorités compétentes de se saisir, le cas échéant, des informations divulguées. On l'a vu dans l'affaire des « *Panama Papers* » et plus récemment dans celle des « *Cambridge Analytica Files* ».

On le voit, le lancement d'alerte souffre d'une certaine dualité, laquelle traverse le droit européen. Nous y reviendrons dans la section suivante.

D. – *L'organisation – administration ou entreprise – concernée par le signalement*

12. Enfin, et c'est là le dernier élément constitutif, la Cour européenne des droits de l'homme distingue selon que le lanceur d'alerte relève du secteur public ou du secteur privé. Si tout travailleur jouit du droit à la liberté d'expression, la juridiction estime en effet que le devoir de réserve auquel est soumis un fonctionnaire de l'État doit être apprécié plus strictement[50].

Ceci étant, la protection des lanceurs d'alerte doit couvrir à la fois le travailleur du secteur public et celui du secteur privé[51]. En pratique, cette protection peut être globale ou sectorielle. Par exemple, au Royaume-Uni, le *Public Interest Disclosure Act* (« PIDA ») protège à la fois les lanceurs d'alerte du secteur public et ceux du secteur privé, alors que, aux États-Unis, le *Whistleblower Protection Act* (« WPA ») ne protège que les fonctionnaires de l'administration fédérale[52].

49 Consulté le 10 juin 2017.

50 Cour eur. D.H., *Guja*, préc., § 70.

51 Voy. not. le document de travail publié par la Commission dans le cadre de la consultation publique sur la protection des lanceurs d'alerte, préc., p. 2 ; résolution du Parlement européen du 24 octobre 2017, préc., pts 1er et T ; recommandation CM/Rec (2014) 7, annexe, définitions, a).

52 Voy. not. 7e rapport général d'activité (2006) du GRECO, adopté lors de la 32e réunion plénière du GRECO, p. 12.

III. L'émergence de la figure du « lanceur d'alerte » en droit européen

13. Ainsi que nous l'avons déjà suggéré, le droit européen repose sur une double conception du lancement d'alerte. Après avoir explicité cette dualité de conception (A), nous l'illustrerons au travers des textes les plus significatifs adoptés en Europe (B) tantôt au sein du Conseil de l'Europe (1), tantôt au sein de l'Union européenne (2).

A. – *La dualité conceptuelle du lancement d'alerte en Europe*

14. La proposition de directive déposée par la Commission européenne le 23 avril dernier se fait encore le témoin de tout l'ambivalence que renferme le concept de lancement d'alerte[53]. Cette dualité nous paraît fondamentale en ce qu'elle explique, d'une part, la variété de régimes juridiques en la matière et, d'autre part, l'ambiguïté des impressions que suscite le lancement d'alerte. Un auteur français exprime cette dualité au travers des concepts de lancement d'alerte « démocratique » et de lancement d'alerte « managérial »[54].

En son sens « démocratique », le lancement d'alerte se conçoit comme une extension de la liberté d'expression, laquelle est protégée juridiquement parce qu'elle constitue, pour reprendre l'expression de la Cour européenne des droits de l'homme, « l'un des fondements essentiels d'une société démocratique, l'une des conditions primordiales de son progrès et de l'épanouissement de chacun »[55]. À cet égard, la Commission européenne souligne la nécessité de protéger les lanceurs d'alerte en tant que sources d'informations des journalistes[56]. Leur protection s'avère cruciale à la sauvegarde du rôle de « chien de garde » des journalistes d'investigation dans les sociétés démocratiques.

53 Proposition de directive du 23 avril 2018, mémorandum explicatif, pp. 1 et 2.

54 J.-Ph. Foegle, « Le lanceur d'alerte dans l'Union européenne : démocratie, management, vulnérabilité(s) », in *Les lanceurs d'alerte. Quelle protection juridique ? Quelles limites ?* (M. Disant et D. Pollet-Panoussis dir.), Issy-les-Moulineaux, Lextenso, 2017, p. 110. Dans le même sens, voy. aussi, W. Vandekerckhove, « Freedom of Expression as the "Broken Promise" of Whistleblower Protection », *La Revue des droits de l'homme*, 2016, n° 10 (en ligne) ; P. Mbongo, « Manning, Snowden... Deux questions sur les "lanceurs d'alerte" », 31 juillet 2013, *The Huffington Post.fr* (consulté le 8 août 2017).

55 Cour eur. D.H. (Gde ch.), 12 septembre 2011, req. n^{os} 28955/06, 28957/06, 28959/06 et 28964/06, *Palomo Sánchez et autres c. Espagne*, § 53. Voy. aussi Cour eur. D.H. (Gde ch.), 7 décembre 1976, req. n° 5493/72, *Handyside c. Royaume-Uni*, § 49.

56 Proposition de directive du 23 avril 2018, considérant n° 33.

En son sens « managérial » ou « monitoire » (de l'anglais « *monitor* »)[57], le lancement d'alerte est encouragé et favorisé dans les hypothèses où il permet de réaliser des objectifs de politique publique, qu'ils soient internationaux, européens ou nationaux. La sensibilité de cette seconde approche tient au fait qu'elle érige la dénonciation au rang de mode de gouvernance. Or, une telle façon de faire était, jusqu'à présent, plutôt l'apanage des régimes totalitaires que des régimes démocratiques.

15. À notre estime, la dualité du concept de lancement d'alerte en Europe s'explique avant tout par son origine. Historique tout d'abord : s'inspirant du *whistleblowing* à l'américaine, le lancement d'alerte renvoie à la faculté – voire le devoir moral ? – de collaborer avec l'État en vue d'assurer l'effectivité des politiques publiques. Prolongement de l'alerte éthique à la française, le lancement d'alerte désigne aussi la liberté de dénoncer les actes contraires à l'intérêt général. Idéologique ensuite : le lancement d'alerte partage avec la dénonciation d'inévitables accointances. Or, la figure du dénonciateur souffre, elle aussi, d'une ambivalence profonde en ce qu'elle renvoie tant au traître qu'au héros.

B. – *L'émergence du statut de « lanceur d'alerte » en droit européen*

16. Le statut de lanceur d'alerte s'est progressivement imposé au sein du Conseil de l'Europe grâce à l'œuvre créatrice de la Cour européenne des droits de l'homme (1), et au sein de l'Union européenne au travers d'une série de textes sectoriels (2).

Eu égard à la définition du lanceur d'alerte proposée ci-dessus, soulignons d'emblée que le signalement public n'est actuellement encadré par aucun texte, mis à part l'article 10 de la CEDH. De façon inédite, la proposition de directive publiée le 23 avril dernier prévoit cependant de protéger aussi les lanceurs d'alerte qui s'adressent au public[58].

1. – *L'émergence du statut de « lanceur d'alerte » au sein du Conseil de l'Europe*

17. Comme on le sait, l'œuvre principale du Conseil de l'Europe demeure la Convention européenne de sauvegarde des droits de l'homme

[57] Voy. not. pour une telle conception « *whistleblower like a monitor* » : B. FASTERLING, « Whistleblower Protection : A Comparative Law Perspective », in *International Handbook on Whistleblowing Research* (D. LEWIS *et al.* éd.), Cheltenham, Elgar, 2014, pp. 340-345.

[58] La révélation publique ne s'est toutefois pas vu accorder la même attention que les signalements interne et externe qui jouissent, quant à eux, d'un chapitre exprès.

et des libertés fondamentales, qui lie tous ses membres. C'est sous l'angle de son article 10, qui consacre le droit à la liberté d'expression, que la Cour européenne des droits de l'homme a développé une jurisprudence protectrice des lanceurs d'alerte. La haute juridiction a, par ailleurs, enrichi son interprétation et son application de l'article 10 de la Convention au moyen de textes très divers, qui relèvent tant du *hard law* (a) que du *soft law* (b)[59].

a) *Le* hard law *du lancement d'alerte*

18. C'est à l'occasion de l'affaire *Guja* que la Cour européenne des droits de l'homme a rendu son premier arrêt, qui constitue un arrêt de principe, en matière de lancement d'alerte. Dans sa décision, la Cour renvoie au cadre juridique international et européen pertinent en matière de lutte contre la corruption. Celui-ci se compose, pour l'essentiel, des conventions pénales et civiles du Conseil de l'Europe sur la corruption[60] et de la Convention des Nations unies contre la corruption dite « Convention de Mérida »[61].

Sans faire expressément référence aux « lanceurs d'alerte », l'article 22 de la Convention pénale du Conseil de l'Europe sur la corruption garantit la protection des collaborateurs de justice et des témoins ». Le pendant civil de la Convention pénale sur la corruption prévoit, quant à lui, en son article 9, une protection des employés qui, de bonne foi et sur la base de soupçons raisonnables, dénoncent des faits de corruption aux personnes ou autorités responsables. Ce texte a sensiblement inspiré les auteurs de la Convention des Nations unies contre la corruption dans la rédaction de l'article 33, qui, rappelons-le, représente, sur la scène internationale, l'un des premiers textes sur le sujet des lanceurs d'alerte[62].

19. À première vue, les deux conventions du Conseil de l'Europe, en ce qu'elles encouragent le signalement d'informations en vue de lutter

59 Sur ce mouvement, voy. F. TULKENS, S. VAN DROOGHENBROECK et F. KRENC, « Le *soft law* et la Cour européenne des droits de l'homme. Questions de légitimité et de méthode », in *Les sources du droit revisitées* (I. HACHEZ *et al.*), vol. I, Limal, Anthemis, 2012, pp. 381-431.

60 Notons qu'une structure a spécialement été créée, le Groupe d'États contre la corruption (GRECO), en vue de veiller au respect, par les États membres, des normes de lutte contre la corruption adoptées par le Conseil de l'Europe. Dans son septième rapport général d'activité (2006), le GRECO a inclu un chapitre complet sur la « Protection des lanceurs d'alerte » (« *Protection of Whistleblowers* »).

61 Convention des Nations unies contre la corruption, préc.

62 À la lumière du *Resource Guide on Good Practices in the Protection of Reporting Persons* (*op. cit.*, p. 89), il est manifeste que l'expression « *reporting persons* », utilisée dans l'art. 33, désigne les « *whistleblowers* » et, partant, les « lanceurs d'alerte ». À cet égard, soulignons que la proposition de directive du 23 avril 2018 a également préféré utiliser, dans le texte de la directive, l'expression « *reporting persons* » plutôt que celle de « *whistleblowers* ».

contre la corruption, semblent plutôt relever de la conception managériale du lancement d'alerte. Cependant, l'accent est clairement mis sur la protection de celui qui signale des informations (conception démocratique) plus que sur les moyens à mettre en œuvre en vue d'encourager le signalement de certains faits (conception managériale).

b) *Le* soft law *du lancement d'alerte*

20. Parmi les textes de *soft law* adoptés par le Conseil de l'Europe, deux textes en particulier méritent notre attention, dès l'instant où la Cour européenne des droits de l'homme s'y est référée, dans le prolongement de l'arrêt *Guja*, pour la construction de sa jurisprudence protectrice.

Dans sa résolution 1729(2010)[63], l'Assemblée parlementaire invite les États membres à passer en revue leur législation sur la protection des lanceurs d'alerte à la lumière d'un certain nombre de principes directeurs. Conscient que bon nombre d'États demeuraient néanmoins sans règles juridiques complètes en la matière, le Comité des ministres est venu, par sa recommandation CM/Rec (2014) 7, « ancrer fermement la protection des lanceurs d'alerte dans le champ des principes démocratiques et de la préservation de l'intérêt général ». La recommandation se garde de prendre position sur l'opportunité d'adopter ou non une loi unique sur la protection des lanceurs d'alerte. L'important est de pouvoir compter sur un « cadre », à savoir une série d'« éléments normatifs, institutionnels et judiciaires qui forment un tout cohérent dans lequel les voies permettant de signaler et de révéler des informations, les mécanismes d'enquête et de réparation, ainsi que les voies de recours juridiques pour la protection des lanceurs d'alerte s'articulent tous efficacement »[64].

21. Dans la mesure où la protection des sources journalistiques, bien établie dans la jurisprudence de la Cour européenne des droits de l'homme[65], assure également la protection des lanceurs d'alerte qui s'adressent à un « journaliste »[66], on mentionnera encore la recomman-

63 Résolution 1729(2010) de l'Assemblée parlementaire du Conseil de l'Europe sur la protection des « donneurs d'alerte », discussion et adoption par l'Assemblée le 29 avril 2010, 17e séance.

64 Recommandation CM/Rec (2014) 7, exposé des motifs, §§ 29 et 50.

65 Voy. not. Cour eur. D.H. (Gde ch.), 27 mars 1996, req. n° 17488/90, *Goodwin c. Royaume-Uni*, § 39 ; Cour eur. D.H. (Gde ch.), 14 septembre 2010, req. n° 38224/03, *Sanoma Uitgevers B.V. c. Pays-Bas*, § 50 ; Cour eur. D.H. (5e sect.), 12 avril 2012, req. n° 30002/08, *Martin et autres c. France*, § 59 ; Cour eur. D.H. (5e sect.), 18 avril 2013, req. n° 26419/10, *Saint-Paul Luxembourg S.A. c. Luxembourg*, § 49. Voy. aussi la recommandation n° R (2000) 7 du Comité des ministres sur le droit des journalistes de ne pas révéler leurs sources d'information.

66 Voy. not. Cour eur. D.H., *Görmüs*, préc., § 60. Pour une critique de cet arrêt, voy. not. Q. VAN ENIS, « Une solide protection des sources journalistiques et des lanceurs d'alerte : une impérieuse nécessité à l'ère dite de la "post-vérité" ? », *op. cit.*, pp. 95-152 ; Q. VAN ENIS, « Un curieux rétrécissement de la

dation CM/Rec (2011) 7 « sur une nouvelle conception des médias » et la recommandation 1950 (2011) sur la « protection des sources d'information des journalistes ». Dès lors que, comme nous l'avons signalé plus haut, le lancement d'alerte passe aujourd'hui presque nécessairement par le truchement d'une interface Web sécurisée, se pose en particulier la question, comme le note l'Assemblée parlementaire, de l'application du droit des journalistes de ne pas divulguer leurs sources d'information lorsque l'interface a été conçue pour la diffusion publique d'informations d'intérêt général. Nous y reviendrons par la suite.

2. – *L'émergence du statut de « lanceur d'alerte » au sein de l'Union européenne*

22. C'est à l'occasion de la mise en œuvre par des entreprises européennes d'un texte américain, le « *Sarbanes-Oxley Act* » (ci-après : « *SOX Act* »), que la problématique de la conformité du *whisteblowing* avec le droit de l'Union européenne s'est posée pour la première fois concrètement[67]. La section 301 de ce texte exige en effet des comités d'audit des entreprises publiques américaines et de leurs filiales dans l'Union européenne, ainsi que des sociétés non américaines cotées à une bourse américaine, d'établir une procédure permettant aux employés de soumettre de façon anonyme leurs inquiétudes au sujet de problèmes dans le domaine de la comptabilité et de l'audit. Parallèlement, la section 806 de ce texte insère expressément un régime de protection selon lequel les employés, contractants, sous-contractants et agents des sociétés cotées ne peuvent faire l'objet de représailles de la part de leur employeur pour avoir révélé auprès d'un supérieur, ou d'une autre autorité compétente telle qu'énumérée légalement, toute conduite dont on peut croire qu'elle constitue une violation des règles de la *Securities and Exchange Commission* (ci-après : « SEC »)[68] ou de toute loi fédérale ayant pour objet les fraudes perpétrées à l'encontre des actionnaires.

23. Forte de la conception managériale du lancement d'alerte véhiculée par le *SOX Act*, l'Union européenne a mis à charge de certaines entités du secteur privé l'obligation de mettre en place des dispositifs

protection des sources : obs. sous Cour européenne des droits de l'homme, 2e sect., arrêt *Gormus et autres c. Turquie*, 19 janvier 2016 », *Journalistes* (mensuel de l'Association des Journalistes Professionnels), 2017, n° 191, p. 2.

67 Sur le dispositif de *whistleblowing* prévu par le *SOX Act*, voy. not. T. M. Dworkin, « SOX and Whistleblowing », *Michigan Law Review*, 2007, vol. 105/8, pp. 1774 et 1775.

68 Précisons que la SEC contrôle l'application du *SOX Act* aux États-Unis.

d'alerte en vue d'assurer l'exécution de certaines politiques publiques (a). Il n'empêche que la conception démocratique n'est nullement exclue au sein de l'Union européenne, mais les textes qui la défendent ne jouissent pas d'une force juridique contraignante (b).

a) *L'instrumentalisation du whistleblowing par le droit de l'Union européenne*

24. En l'état actuel du droit[69], l'obligation d'instaurer un dispositif d'alerte interne existe, pour le secteur privé, dans la plupart des États membres de l'Union européenne en vue de mieux réguler le secteur bancaire[70], de lutter contre les abus de marché[71], contre le blanchiment de capitaux et le financement du terrorisme[72] et de garantir la sécurité des opérations pétrolières et gazières en mer[73] ainsi que des transports maritimes[74] et des transports en avion[75]. À la lecture de la proposition de directive du 23 avril dernier, on peut du reste s'attendre à la création d'une telle obligation dans bien d'autres domaines relevant du droit de l'Union[76], notamment dans le domaine de la lutte contre la

69 Pour une recension de la règlementation internationale et européenne existante, voy. not. F. COTON et J.-Fr. HENROTTE, « Le lanceur d'alerte : une personne concernée par le traitement de ses données à caractère personnel, mais également par son avenir professionnel… », *R.D.T.I.*, 2015, n° 61, pp. 45-55.

70 Directive 2013/36/UE du Parlement européen et du Conseil du 26 juin 2013 concernant l'accès à l'activité des établissements de crédit et la surveillance prudentielle des établissements de crédit et des entreprises d'investissement, modifiant la directive 2002/87/CE et abrogeant les directives 2006/48/CE et 2006/49/CE, *J.O.U.E.*, L 176/338 à L 176/436, 27 juin 2013 (directive bancaire) et directive 2009/138/CE du Parlement européen et du Conseil du 25 novembre 2009 sur l'accès aux activités de l'assurance et de la réassurance et leur exercice (Solvabilité II), *J.O.U.E.*, L 335/1 à L 335/155, 17 décembre 2009 (directive Solvabilité II).

71 Règlement (UE) n° 596/2014 du Parlement européen et du Conseil du 16 avril 2014 sur les abus de marché et abrogeant la directive 2003/6/CE du Parlement européen et du Conseil et les directives 2003/124/CE, 2003/125/CE et 2004/72/CE de la Commission, *J.O.U.E.*, L 173/1 à L 173/61, 12 juin 2014.

72 Directive (UE) 2015/849 du Parlement européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission, *J.O.U.E.*, L 141/73 à L 141/117, 5 juin 2015 (quatrième directive anti-blanchiment).

73 Directive (UE) 2013/30/UE du Parlement européen et du Conseil du 12 juin 2013 relative à la sécurité des opérations pétrolières et gazières en mer et modifiant la directive 2004/35/CE, *J.O.U.E.*, L 178/66 à L 178/106, 28 juin 2013, art. 22, considérant n° 41 et annexe IV.

74 Directive 2013/54/UE du Parlement européen et du Conseil du 20 novembre 2013 relative à certaines responsabilités de l'État du pavillon en ce qui concerne le respect et la mise en application de la Convention du travail maritime, 2006, *J.O.U.E.*, L 329/1 à L 329/4, 10 décembre 2013 et directive 2009/16/CE du Parlement européen et du Conseil du 23 avril 2009 relative au contrôle par l'État du port, *J.O.U.E.*, L 131/57 à L 131/100, 28 mai 2009, art. 23.5.

75 Règlement (UE) n° 376/2014 du Parlement européen et du Conseil du 3 avril 2014 concernant les comptes rendus, l'analyse et le suivi d'événements dans l'aviation civile, modifiant le règlement (UE) n° 996/2010 du Parlement européen et du Conseil et abrogeant la directive 2003/42/CE du Parlement européen et du Conseil et les règlements de la Commission (CE) n° 1321/2007 et (CE) n° 1330/2007, *J.O.U.E.*, L 122/18 à L 122/43, 24 avril 2014, art. 4 et 5.

76 Conformément au principe de proportionnalité, la proposition de directive du 23 avril 2018 n'établit des standards minimum communs de protection que dans certains domaines de politique. Ceux-ci ont été sélectionnés sur la base de trois critères, selon i) qu'il existe un besoin de renforcer l'effectivité du droit en

fraude et l'évasion fiscales, conformément au rapport de la Commission PANA[77].

À l'instar des obligations prévues par le *SOX Act*, les obligations ici prescrites vont de pair avec l'obligation de prévoir des mesures de protection des personnes ayant recours au dispositif d'alerte.

25. Le secteur public n'est, quant à lui, actuellement affecté que dans un seul domaine, celui de la lutte contre la corruption. Ce domaine n'est régulé par aucun texte de *hard law* en droit de l'Union[78], mais la plupart des États membres se sont dotés d'une législation nationale sur le sujet[79]. La proposition de directive du 23 avril 2018 aurait donc pour conséquence de considérablement élargir les obligations dans le secteur[80].

26. Parmi les règlementations spécifiques adoptées par l'UE, le Règlement sur les abus de marché occupe une place singulière en ce sens qu'il représente, aux yeux du Parlement européen, le principal texte apte à fonder juridiquement, en droit de l'Union, le lancement d'alerte[81]. En particulier, soulignons que l'article 32 de ce Règlement, qui est inspiré d'un texte américain, le *Dodd-Frank Act*[82], autorise

question ; ii) que la pauvreté des signalements est un facteur clé qui affecte l'effectivité du droit en question ; iii) que les manquements au droit de l'Union peuvent résulter en des atteintes sérieuses à l'intérêt public (mémorandum explicatif, p. 6 et considérant n° 5).

77 Committee of Inquiry to investigate alleged contraventions and maladministration in the application of Union law in relation to money laundering, tax avoidance and tax evasion (Commission PANA), report on the inquiry into money laundering, tax avoidance and tax evasion (2017/2013[INI]), 16 novembre 2017, §§ 171-174. Dans le même sens, voy. le rapport de la Commission belge « Panama Papers » (rapport fait au nom de la Commission spéciale « Fraude fiscale internationale/Panama Papers » : Les *Panama Papers* et la fraude fiscale internationale, 31 octobre 2017, *doc. parl.*, Ch. repr., sess. ord. 2017-2018, n° 54-2749/001, recommandation n° 23, p. 28).

78 Sur le sujet, les instances européennes renvoient elles-mêmes aux travaux de l'ONU, du Conseil de l'Europe et de l'OCDE. Voy. not. le rapport anticorruption de l'UE, 3 février 2014, COM(2014) 38 final. Soulignons que ces textes visent tant les travailleurs du secteur public que du secteur privé.

79 Par exemple, voy., en Belgique, la loi du 15 septembre 2013 relative à la dénonciation d'une atteinte suspectée à l'intégrité au sein d'une autorité administrative fédérale par un membre de son personnel, *M.B.*, 4 octobre 2013. La France a, de son côté, choisi de se limiter, dans un premier temps, aux travailleurs du secteur privé (art. 9 de la loi française n° 2007-1598 du 13 novembre 2007 relative à la lutte contre la corruption, *J.O.R.F.*, 14 novembre 2007, n° 264). Néanmoins, la loi Sapin II est venue ériger en France un véritable régime juridique général de protection des lanceurs d'alerte. Sur le sujet, voy. not. A. Lachapelle, « La déclaration d'informations ("*reporting*") comme outil de lutte contre la criminalité financière : commentaire de la décision n° 2016-741 du Conseil constitutionnel français », *T.F.R.*, mai 2017, n° 522, pp. 427-431.

80 L'art. 1er de la proposition de directive du 23 avril 2018 et son annexe (part I et II) énumèrent les multiples domaines de politique pour lesquels les moyennes et grandes entreprises ainsi que les administrations fédérales, régionales et, le cas échéant, communales, doivent établir des canaux de signalement interne.

81 Résolution du Parlement européen du 16 décembre 2015 contenant des recommandations à la Commission en vue de favoriser la transparence, la coordination et la convergence des politiques en matière d'impôt sur les sociétés au sein de l'Union (2015/2010[INL]), recommandation A7 ; résolution du Parlement européen du 14 février 2017 sur le rôle des lanceurs d'alerte dans la protection des intérêts financiers de l'Union européenne (2016/2055[INI]), pt 33. Voy. aussi Groupe des Verts/ALE du Parlement européen, Whistleblower protection in the public and private sector in the European Union. Draft directive, préc., pt 1.8.

82 Le *Dodd-Frank Act* permet à la SEC d'octroyer dans certaines circonstances des récompenses financières aux lanceurs d'alerte (*Dodd-Frank Wall Street Reform and Consumer Protection Act*, adopté le 21 juillet 2010).

l'octroi d'incitations financières aux personnes qui signalent des violations du Règlement. De la sorte, le Règlement ouvre la voie, selon certains observateurs, à la généralisation, en Europe, de l'établissement d'incitants financiers au signalement d'informations[83]. Cette façon de faire est assez commune aux États-Unis. Ainsi, on signalera que l'entreprise américaine Facebook a décidé de créer tout récemment, en réaction directe au scandale de *Cambridge Analytica*, un « programme de signalement d'abus de données basé sur un système de récompenses » dans le but de l'aider à protéger les données de ses utilisateurs. Les cas qui se révèlent fondés peuvent mener à l'octroi d'une récompense de 500 USD au minimum[84]. La presse évoque un montant maximum de 40.000 USD[85].

b) *La protection du lanceur d'alerte au sein de l'Union européenne*

27. Le Parlement européen, fervent défenseur des lanceurs d'alerte, a longtemps invité la Commission à présenter une proposition législative visant à mettre en place un programme européen efficace et complet pour protéger les lanceurs d'alerte[86]. Il encourage également les États membres à assurer une protection adéquate et efficace en droit interne[87].

Soucieuse de répondre aux sollicitations du Parlement[88], la Commission européenne a lancé une consultation publique sur la protection des lanceurs d'alerte du 3 mars 2017 au 29 mai 2017[89]. Cette consultation visait principalement à se prononcer sur le choix d'un

83 Voy. not. B. FASTERLING, « Whistleblower Protection : A Comparative Law Perspective », *op. cit*., p. 343.

84 *Data Abuse Bounty Program*, Questions/Réponses, www.facebook.com (consulté le 12 avril 2018).

85 Voy. not. C. NGUYEN, « Facebook Will Offer you $40,000 to Find the Next Cambridge Analytica », 10 avril 2018, *Digital Trends*, https://www.digitaltrends.com (consulté le 12 avril 2018) ; A. NG, « Facebook Launches Bug Bounty Program to Report Data Thieves », *CNet.com*, https://www.cnet.com (consulté le 12 avril 2018).

86 Voy. not. la résolution du Parlement européen du 23 octobre 2013 sur la criminalité organisée, la corruption et le blanchiment de capitaux : recommandations sur des actions et des initiatives à entreprendre (rapport final), 2013/2107(INI), pt 14 ; résolution du Parlement européen du 25 novembre 2015 sur les rescrits fiscaux et autres mesures similaires par leur nature ou par leur effet (2015/2066[INI]) (TAXE 1), pt 144 ; résolution du Parlement européen du 16 décembre 2015 contenant des recommandations à la Commission en vue de favoriser la transparence, la coordination et la convergence des politiques en matière d'impôt sur les sociétés au sein de l'Union (2015/2010[INL]), recommandation A7 ; résolution du Parlement européen du 6 juillet 2016 sur les rescrits fiscaux et autres mesures similaires par leur nature ou par leur effet (2016/2038[INI]) (TAXE 2), pt 46 ; résolution du Parlement européen du 14 février 2017 sur le rôle des lanceurs d'alerte dans la protection des intérêts financiers de l'Union européenne (2016/2055[INI]), pt 2 ; résolution du Parlement européen du 24 octobre 2017, préc., pt F.

87 Voy. not. la résolution du Parlement européen du 23 octobre 2013, préc., pts 14 et 73 ; résolution du Parlement européen du 14 février 2017, préc., pts 6-8.

88 Commission européenne, « Justice fiscale : la Commission présente les prochaines mesures visant à accroître la transparence fiscale et à lutter contre les pratiques fiscales abusives », communiqué de presse, Strasbourg, 5 juillet 2016.

89 « Public consultation on *whistleblower* protection », http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=54254 (consulté le 8 mars 2017).

instrument général horizontal ou sur le maintien d'instruments sectoriels, et sur le contenu d'un instrument horizontal, le cas échéant. À l'issue de cette consultation, la Commission s'est dirigée vers la rédaction d'un instrument horizontal qu'elle a présenté le 23 avril dernier. Prenant acte de la dualité fondamentale qui caractérise le lancement d'alerte – à la fois exercice de la liberté d'expression et outil d'exécution du droit – ce texte a pour objectif d'exploiter au maximum le potentiel de la protection des lanceurs d'alerte, en établissant une série de standards communs minimums, afin de renforcer l'effectivité du droit de l'Union européenne dans certains domaines de politiques spécifiques[90]. Il découle de la lecture des nombreux considérants consacrés sur le sujet que la protection des données à caractère personnel, et spécialement l'exigence de confidentialité, occupe une place cardinale dans le régime européen de protection des lanceurs d'alerte[91]. Erigé au rang de droit fondamental par l'article 8 de la Charte des droits fondamentaux de l'Union européenne, la protection des données représente de fait une préoccupation majeure en Europe. En témoigne encore la mise en application du Règlement général sur la protection des données (ci-après « RGPD »). En l'occurrence, rappelons que c'est avec ce droit, et à celui à la vie privée, que le *whistleblowing* américain s'est tout d'abord heurté en Europe[92].

IV. La protection du lanceur d'alerte en droit européen des droits de l'homme

28. La recommandation (2014) 7 du Comité des ministres prévoit une protection des lanceurs d'alerte « contre toutes formes de représailles, directes ou indirectes, de la part de leur employeur et de la part de personnes travaillant pour le compte ou agissant au nom de cet employeur »[93]. La recommandation ne précise pas la forme précise que

90 Proposition de directive du 23 avril 2018, mémorandum explicatif, p. 1, considérant n° 1, art. 1 et annexe (part I et II).

91 Proposition de directive du 23 avril 2018, considérants nos 43, 44, 48, 53, 55, 58, 79 et 85 et l'art. 18. Voy. aussi art. 32, 2, c), du règlement (UE) n° 596/2014 sur les abus de marché ; considérants nos 41 et 43 de la quatrième directive anti-blanchiment et communication de la Commission au Parlement européen, au Conseil et au Comité économique et social européen, La lutte contre la corruption dans l'Union européenne, 6 juin 2011, COM(2011) 308 final, p. 13, pt 4.1.3.

92 Voy. not. C. Kuner, *European Data Protection Law. Corporate Compliance and Regulation*, 2e éd., Oxford, OUP, 2007, p. 271.

93 Recommandation CM/Rec (2014) 7, annexe, section VII, principe 21.

devrait prendre cette protection. Il incombe aux États membres de la définir en fonction de leurs principes juridiques[94].

En tout état de cause, le lanceur d'alerte bénéficie de la protection des droits de l'homme. Cette protection implique un délicat équilibre entre deux valeurs à la fois opposées et complémentaires : la transparence et le secret.

29. Alors que la valeur de la transparence se trouve incarnée par le droit à la liberté d'expression (A), la valeur du secret est, quant à elle, protégée via le droit au respect de la vie privée (B). À la croisée de ces droits fondamentaux se trouvent les droits au chiffrement et à l'anonymat (C). Outils fondamentaux de sécurisation des activités en ligne, ces droits s'avèrent être, dans les faits, un premier rempart efficace contre les représailles.

A. – *La protection du lanceur d'alerte sous l'angle de la liberté d'expression*

30. La Cour européenne des droits de l'homme a reconnu, sous le prisme du droit à la liberté d'expression, le droit des travailleurs de signaler les conduites ou actes illicites constatés sur leur lieu de travail (1). En vue d'examiner le respect de ce droit, elle a développé une jurisprudence spécifique au départ de son arrêt *Guja* (2). Par ailleurs, il s'avère que le lanceur d'alerte peut représenter, dans certaines circonstances, une « source journalistique » et, partant, bénéficier de la protection attachée à une telle source d'information (3).

1. – *Le droit de dénoncer des actes répréhensibles*

31. Entendu comme une extension du droit à la liberté d'expression, le droit de dénoncer des irrégularités appartient à tout citoyen, que celui-ci agisse dans le cadre de sa relation de travail[95] ou non[96], qu'il s'exprime directement en ayant recours, ou non, aux outils numériques, ou indirectement, notamment en s'adressant aux autorités[97], à

94 *Ibid.*, exposé des motifs, § 83.

95 Voy. Cour eur. D.H., *Heinisch*, préc., § 43.

96 Voy. Cour eur. D.H. (2e sect.), 15 novembre 2012, req. nos 53579/09 et 53582/09, *Bargão et Domingos Correia c. Portugal*, § 35.

97 Voy., s'agissant de la conduite de fonctionnaires : Cour eur. D.H. (5e sect.), 5 octobre 2006, n° 14881/03, *Zakharov c. Russie*, § 23 ; Cour eur. D.H. (5e sect.), 31 mars 2011, req. n° 6428/07, *Siryk c. Ukraine*, § 42 ; Cour eur. D.H. (5e sect.), 21 décembre 2010, req. n° 34690/05, *Sofranschi c. Moldova*, § 29 ;

un homme politique[98] ou en passant par l'intermédiaire d'un journaliste[99]. Eu égard au thème qui nous occupe, soulignons que la Cour de Strasbourg a fait de l'accès à Internet une composante intégrante de la liberté d'expression[100].

La « possibilité pour les citoyens de faire part aux agents de l'État compétents d'une conduite qui leur paraît irrégulière ou illicite de la part de fonctionnaires » bénéficie d'une attention spéciale dans la jurisprudence de la Cour dès lors que cette possibilité constitue « l'un des principes de l'état de droit »[101]. Dans l'affaire *Zakharov*, la Cour a, par exemple, admis, au regard de l'article 10 de la CEDH, qu'un citoyen dénonce, par voie de correspondance privée, auprès du vice-gouverneur de la région de Moscou, la conduite irrégulière d'un fonctionnaire déterminé. La juridiction européenne a également reconnu que des ONG pouvaient dénoncer publiquement des irrégularités alléguées dans la conduite d'agents de l'État[102]. Dans ce cas, l'ONG exerce « un rôle de chien de garde public semblable par son importance à celui de la presse »[103]. Il en découle alors une appréciation plus stricte des « devoirs et responsabilités » inhérents à l'exercice de la liberté d'expression[104].

Enfin, ainsi que nous l'avons annoncé, la Cour de Strasbourg a spécifiquement reconnu le droit de dénonciation aux « fonctionnaires et autres salariés »[105], lesquels bénéficient, sous certaines conditions, d'une protection particulière en leur qualité de « lanceur d'alerte » (voy. *infra*, n^os^ 33 et s.).

32. S'agissant de la portée matérielle du droit de dénoncer, on notera que ce droit n'emporte pas, d'après la juridiction strasbourgeoise, le droit de recevoir une réponse quant à la suite donnée aux faits dénoncés, qui plus est positive[106]. En revanche, lorsqu'un dispositif d'alerte est mis en place au sein de l'organisation du travailleur, ou auprès d'une

Cour eur. D.H. (5e sect.), 8 avril 2010, req. n° 10941/03, *Bezymyannyy c. Russie*, § 41 ; Cour eur. D.H. (5e sect.), 18 décembre 2008, req. n° 1758/02, *Kazakov c. Russie*, § 28.

98 Voy. not. Cour eur. D.H., *Zakharov*, préc., § 8.

99 Recommandation 1950 (2011) de l'Assemblée parlementaire du Conseil de l'Europe « sur la protection des sources journalistiques », § 9.

100 Cour eur. D.H. (5e sect.), 19 février 2013, req. n° 40397/12, *Neij et Sunde Kolmisoppi c. Suède* (déc.).

101 Voy. not. Cour eur. D.H., *Zakharov*, préc., § 26 ; *Siryk*, préc., § 42 ; *Sofranschi*, préc., § 30 ; *Bezymyannyy*, préc., § 40 ; *Kazakov*, préc., § 28.

102 En l'occurrence, le signalement portait sur le non-respect du principe de représentation proportionnelle des communautés ethniques dans la procédure de nomination d'un directeur pour la radio publique multiethnique du district et sur la proposition qui s'ensuivait de désigner M.S. au poste de directeur.

103 Cour eur. D.H., *Medzlis*, préc., § 86.

104 *Ibid.*, § 87.

105 Cour eur. D.H., *Guja*, préc., § 97. Voy. aussi Cour eur. D.H., *Heinisch*, préc., §§ 43 et 93 ; *Bucur*, préc., § 120 ; (5e sect), 19 février 2009, req. n° 4063/04, *Marchenko c. Ukraine*, § 46 ; *Bathellier* (déc.), préc.

106 Cour eur. D.H., *Bathellier* (déc.), préc.

autorité compétente, le lanceur d'alerte devrait jouir, d'après le Comité des ministres du Conseil de l'Europe et la Commission européenne, du droit de savoir ce qu'il advient de son signalement ainsi que les suites qui y sont données[107]. En Belgique, l'autorité nationale de protection des données tire, en outre, ce droit des règles de protection des données à caractère personnel (voy. *infra*, n° 63)[108].

2. – *La protection des lanceurs d'alerte*

33. C'est au stade de l'examen du principe de proportionnalité[109] que la spécificité du lancement d'alerte prend forme dans l'examen de la Cour européenne des droits de l'homme. La Cour a défini, à l'occasion de cet exercice, une série de principes visant à définir si, en l'espèce, le travailleur doit être, ou non, protégé sous l'angle de la Convention, en ce qu'il a agi en tant que « lanceur d'alerte ». Ces principes tendent à établir une pondération entre les intérêts des diverses parties en jeu (lanceur d'alerte, personne mise en cause, organisation impliquée, tiers éventuels).

Nous proposons de détailler ces principes de protection dans les lignes qui suivent (b) après avoir émis quelques considérations générales sur leur portée (a).

a) *Considérations générales à propos des principes de protection des lanceurs d'alerte*

34. Développés, dans l'arrêt *Guja*, à la lumière du droit et de la pratique pertinente relatifs au lancement d'alerte dans le domaine de la corruption[110] et du droit du travail[111], les principes de protection des lanceurs d'alerte ont été précisés à la lumière des avancées récentes en

107 Recommandation CM/Rec (2014) 7, annexe, section VI, principe 20. Voy. aussi résolution du Parlement européen du 24 octobre 2017, préc., pt 32 ; proposition de directive du 23 avril 2018, art. 5.1, d) (signalement interne), 6.2, b), 6.3 et 9.1, b) (signalement externe). Voy. aussi considérant n° 46 (signalement interne) et considérants n^{os} 49 et 50 (signalement externe).

108 CPVP, recommandation n° 01/2006 du 29 novembre 2006 relative à la compatibilité des systèmes d'alerte interne professionnelle avec la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel (ci-après « recommandation n° 01/2006 »), p. 6.

109 Pour rappel, la structure d'analyse de la Cour européenne des droits de l'homme est la suivante. Dans un premier temps, elle vérifie si les faits allégués sont susceptibles de représenter une « ingérence ». Le cas échéant, elle examine alors si ladite ingérence est « prévue par la loi », si elle poursuit l'une ou l'autre finalité légitime énumérée au second paragraphe de l'art. 10 de la Convention, et enfin, si elle est « nécessaire dans une société démocratique » afin d'accomplir ces finalités.

110 À savoir, la Convention des Nations unies, les Conventions pénale et civile du Conseil de l'Europe (voy. *supra*, n° 18), ainsi que la recommandation n° (2000)10 du Comité des ministres sur les codes de conduite pour les agents publics.

111 Convention n° 158 de l'Organisation internationale du travail sur le licenciement.

la matière, en particulier la résolution 1729(2010)[112] et la recommandation (2014) 7[113], qui ont toutes deux une portée générale. En outre, bien que pensés dans une affaire qui mettait en jeu un fonctionnaire, ces principes ont, par la suite, été appliqués dans le secteur privé au motif que le devoir de réserve, de discrétion et de loyauté y est, de toute façon, apprécié plus souplement[114].

En revanche, ces principes demeurent actuellement limités au signalement public d'informations, qui ne représente qu'un volet du lancement d'alerte ainsi que nous l'avons vu (voy. *supra*, n° 10)[115]. De fait, les litiges qui ont été portés devant la juridiction strasbourgeoise revêtaient tous une certaine publicité. Dans les affaires *Heinisch* et *Marchenko*, le lanceur d'alerte avait certes signalé les faits auprès des autorités pénales, et non auprès de journalistes, mais il avait également rendu publiques ses allégations par la diffusion de tracts et l'organisation d'une manifestation avec son syndicat. Ceci étant, la Cour précise, dans son arrêt *Heinisch*, qu'une plainte pénale s'analyse déjà en soi « en une dénonciation [*whistle-blowing*] d'un comportement prétendument illicite imputable à l'employeur de l'intéressée et que cet acte relève de l'article 10 de la Convention »[116].

35. Les principes de protection des lanceurs trouvent désormais à s'appliquer en dehors du Palais des droits de l'homme. Le Comité des ministres du Conseil de l'Europe et le rapporteur spécial de l'ONU renvoient ainsi tous deux aux principes de l'arrêt *Guja* pour apprécier la légitimité d'une restriction imposée à la révélation publique d'informations[117]. Ces principes ont de surcroît inspiré le contenu de la proposition de directive déposée par la Commission européenne le 23 avril dernier[118]. Le tribunal de la fonction publique de l'UE n'avait par ailleurs pas hésité, il y a quelques années de cela, à s'appuyer sur les enseignements de l'arrêt *Guja* en vue d'apprécier, au regard de l'article 10 de la CEDH, la légalité d'une sanction d'avertissement par écrit infligée à un

112 Cour eur. D.H., *Heinisch* et *Bucur*.
113 Cour eur. D.H., *Medzlis*.
114 En l'occurrence, les lanceurs d'alerte travaillaient dans une société détenue par l'État, mais dans laquelle la relation entre l'employeur et ses employés obéissait aux règles de droit privé. Dans l'affaire *Heinisch*, la maison de retraite dont les pratiques étaient dénoncées était détenue principalement par le *Land* de Berlin. Et dans l'affaire *Bathellier*, le requérant était le directeur d'un centre EDF-GDF (Loir-et-Cher) sachant que EDF-GDF était, au moment des faits, un établissement public à caractère industriel et commercial.
115 En ce sens, voy. recommandation CM (2017) 7, exposé des motifs, § 53 ; rapport préc., A/70/361, p. 19, § 37.
116 Cour eur. D.H., *Heinisch*, préc., § 43.
117 Recommandation CM (2017) 7, exposé des motifs, § 53 ; rapport préc., A/70/361, p. 19, § 37.
118 Proposition de directive du 23 avril 2018, considérant n^os^ 23 et 61 et mémorandum explicatif, p. 10. Voy. aussi résolution du Parlement européen du 24 octobre 2017, préc., pt AH.

fonctionnaire de la Cour de justice[119]. Le tribunal a néanmoins conclu au rejet du recours au motif que les deux courriels envoyés par la requérante à l'ensemble des membres de son unité de travail contenaient des accusations graves et des propos virulents contre des personnes identifiées. Aussi, ils ne constituaient pas une voie appropriée de dénonciation eu égard aux voies prévues légalement par les articles 22*bis* et 22*ter* du statut de la Cour de justice[120].

36. À la lumière de l'actualité récente, on notera enfin que la poursuite de mesures de représailles, alors qu'un arrêt a été rendu par la Cour européenne des droits de l'homme, peut constituer une nouvelle violation de l'article 10 de la Convention. Dans son second arrêt *Guja*, la Cour européenne des droits de l'homme a ainsi jugé que le second licenciement du lanceur d'alerte, qui faisait suite à sa réintégration au sein du Parquet général, ne s'apparentait pas à un conflit ordinaire de travail, mais avait toutes les caractéristiques d'un nouvel acte de représailles perpétré en conséquence de l'acte de *whistleblowing* que ce dernier avait posé en 2003, lequel avait donné lieu au premier arrêt *Guja* de la Cour[121]. Faisant application des critères développés à l'occasion de ce premier arrêt, la juridiction européenne a particulièrement été attentive au fait que les juridictions nationales n'avaient nullement examiné les allégations du requérant relatives à la violation de son droit à la liberté d'expression[122].

b) *Examen des principes de protection des lanceurs d'alerte*

37. Selon les principes dégagés par la Cour européenne des droits de l'homme[123], la divulgation au public ne doit intervenir qu'en dernier ressort (1). L'information publiée doit ensuite présenter un intérêt public (2)

119 Tribunal de la fonction publique (3e chambre), 5 décembre 2012, aff. jointes F-88/09 et F-48/10, *Z. c. Cour de justice de l'Union européenne*, §§ 245-255.

120 La requérante a introduit un pourvoi en cassation contre la décision du tribunal de la fonction publique mais elle n'y a pas repris son moyen relatif à l'art. 10 de la CEDH. De plus, celui-ci a été rejeté en grande partie (tribunal (chambre des pourvois), 19 juin 2015, aff. T-88/13 P, *Z c. Cour de justice de l'Union européenne*).

121 Cour eur. D.H. (2e sect.), 27 février 2018, req. n° 1085/10, *Guja c. Moldavie (n° 2)*, §§ 57 et 58.

122 Cour eur. D.H., *Guja (n° 2)*, préc., §§ 59 et 60.

123 Sur ces principes, voy. not. Q. VAN ENIS, « Une solide protection des sources journalistiques et des lanceurs d'alerte : une impérieuse nécessité à l'ère dite de la "post-vérité" ? », *op. cit.*, pp. 95-151 ; V. JUNOD, « Lancer l'alerte : quoi de neuf depuis Guja ? (Cour eur. dr. h., *Bucur et Toma c. Roumanie*, 8 janvier 2013) », *Rev. trim. D.H.*, 2014, vol. 98, pp. 459-482 ; K. ROSIER, « Chapitre III : Hypothèses dans lesquelles une violation des obligations de secret ou de confidentialité pourrait être admise, Section 1. *Whistleblowing* », in *Secret et loyauté dans la relation de travail* (S. GILSON, K. ROSIER, A. ROGER et S. PALATE dir.), Waterloo, Kluwer, 2013, pp. 129-150 ; V. JUNOD, « La liberté d'expression du whistleblower. Cour européenne des droits de l'homme (Grande chambre), *Guja c. Moldova*, 12 février 2008 », *op. cit.*, pp. 227-260.

et être authentique (3) ; le dénonciateur doit agir de bonne foi (4) ; l'intérêt du public d'obtenir l'information dénoncée doit peser plus lourd que le dommage supporté par l'employeur (5) ; enfin, la gravité de la sanction encourue par le dénonciateur est prise en considération par le juge (6).

Les principes établis par la Cour européenne sont cumulatifs bien que certains semblent occuper une place prépondérante, tel que celui relatif à l'existence d'autres moyens de divulgation[124], qui est placé systématiquement en tête[125] ou mis en exergue par la Cour elle-même[126].

i. – *L'existence d'autres moyens pour procéder à la divulgation*

38. Suivie en ce sens par le Comité des ministres du Conseil de l'Europe[127] et la Commission européenne[128], la Cour européenne des droits de l'homme défend le suivi d'une procédure échelonnée eu égard au devoir de loyauté, de réserve et de discrétion auquel est astreint le lanceur d'alerte[129]. Il importe que ce dernier « procède à la divulgation d'abord auprès de son supérieur ou d'une autre autorité ou instance compétente. La divulgation au public ne doit être envisagée qu'en dernier ressort, en cas d'impossibilité manifeste d'agir autrement »[130]. La formulation alternative utilisée s'agissant du signalement interne et du signalement externe ne doit pas tromper : en principe, le lanceur d'alerte doit, d'abord, faire part de ses préoccupations en interne, au sein de son entreprise ou de son administration, avant de les signaler en externe aux autorités[131].

39. La procédure échelonnée que préconise la juridiction européenne n'est néanmoins pas absolue. Une appréciation au cas par cas plutôt qu'une hiérarchie stricte entre les canaux de signalement doit être préférée[132]. S'il n'existe pas de dispositif d'alerte permettant de faire

124 Q. Van Enis, « Une solide protection des sources journalistiques et des lanceurs d'alerte : une impérieuse nécessité à l'ère dite de la "post-vérité" ? », *op. cit.*, pp. 131 et 132, n° 47.

125 Cour eur. D.H., *Heinisch*, préc., § 65 ; *Guja*, préc., § 73 ; *Bucur*, préc., §§ 97-100.

126 Cour eur. D.H., *Medzlis*, préc., § 80.

127 Recommandation CM/Rec (2014) 7, exposé des motifs, § 67.

128 Proposition de directive du 23 avril 2018, art. 13.

129 Sur cette procédure échelonnée, voy. not. V. Junod, « Lancer l'alerte : quoi de neuf depuis Guja ? (Cour eur. dr. h., *Bucur et Toma c. Roumanie*, 8 janvier 2013) », *op. cit.*, p. 468 ; *id.*, « La liberté d'expression du whistleblower. Cour européenne des droits de l'homme (Grande chambre), *Guja c. Moldova*, 12 février 2008 », *op. cit.*, pp. 227-260 ; K. Rosier, « Chapitre III : Hypothèses dans lesquelles une violation des obligations de secret ou de confidentialité pourrait être admise, Section 1. *Whistleblowing* », *op. cit.*, p. 134.

130 Cour eur. D.H., *Heinisch*, préc., § 65 ; *Guja*, préc., § 73.

131 Q. Van Enis, « Une solide protection des sources journalistiques et des lanceurs d'alerte : une impérieuse nécessité à l'ère dite de la "post-vérité" ? », *op. cit.*, p. 132, pt 49. Pour une illustration, voy. not. Cour eur. D.H., *Bathellier* (déc.), préc. ; Cour eur. D.H., *Heinisch*, préc., §§ 73-76 ; Cour eur. D.H. (5e sect.), 21 juin 2016, req. n° 79972/12, *Soares c. Portugal*, § 48.

132 Voy. not. recommandation CM/Rec (2014) 7, exposé des motifs, § 67 ; résolution du Parlement européen du 24 octobre 2017, préc., pt 34 ; proposition de directive du 23 avril 2018, mémorandum explicatif, p. 12 et considérants n° 61-64.

part de ses préoccupations en interne, ou si celui-ci s'avère inefficace ou inadapté compte tenu de la nature du problème, le lanceur d'alerte pourrait légitimement, sans perdre le bénéfice de sa protection, passer directement à l'échelon externe[133]. D'où l'importance pour une organisation de disposer de canaux de signalement interne clairs et efficaces[134]. De surcroît, des circonstances exceptionnelles, telles que la violation grave du droit international des droits de l'homme, du droit international humanitaire ou d'autres droits fondamentaux par un État, ou le risque d'un danger irréversible, peuvent nécessiter de recourir directement à la divulgation au public[135].

Dans l'affaire *Bucur*, la Cour a ainsi observé que le Gouvernement roumain n'avait produit aucun élément démontrant l'existence, à l'époque des faits[136], de dispositions concernant la divulgation par des employés d'irrégularités commises sur leur lieu de travail[137]. De plus, il était manifeste que les irrégularités observées par le lanceur d'alerte (interceptions illégales de conversations téléphoniques au sein du service de renseignement dans lequel il travaillait) concernaient directement ses supérieurs. Il s'ensuit que, dans les circonstances de l'espèce, une divulgation directement à l'opinion publique pouvait se justifier.

ii. – *L'intérêt public présenté par les informations divulguées*

40. Exigence classique dans le contexte de la liberté de la presse[138], le critère de l'intérêt public rappelle que la jurisprudence de la Cour de Strasbourg a spécialement été construite en ayant égard à la divulgation publique d'informations[139], même si le lancement d'alerte englobe également le signalement interne et le signalement externe.

133 En ce sens, voy. not. recommandation CM/Rec (2014) 7, exposé des motifs, § 67 ; résolution du Parlement européen du 24 octobre 2017, préc., pt 34 ; proposition de directive du 23 avril 2018, art. 13.2.

134 La proposition de directive déposée par la Commission européenne le 23 avril dernier vise à l'obliger dans de nombreux cas (voy. not. considérant nos 61 et 62).

135 En ce sens, voy. proposition de directive du 23 avril 2018, art. 13.4 ; rapport préc., A/70/361, p. 19, § 38. Voy. aussi la loi française « Sapin II », dont l'art. 8, III, prévoit qu'« en cas de danger grave et imminent ou en présence d'un risque de dommages irréversibles », le signalement peut intervenir directement auprès d'autorités externes ou être rendu public. Sur le sujet, voy. not. A. LACHAPELLE, « La déclaration d'informations ("*reporting*") comme outil de lutte contre la criminalité financière : commentaire de la décision n° 2016-741 du Conseil constitutionnel français », *op. cit.*, pp. 427-431.

136 Depuis lors, la Roumanie s'est dotée d'une loi relative aux lanceurs d'alerte dans le secteur public (loi n° 571/2004).

137 Cour eur. D.H, *Bucur*, préc., §§ 96 et 97.

138 Q. VAN ENIS, « Une solide protection des sources journalistiques et des lanceurs d'alerte : une impérieuse nécessité à l'ère dite de la "post-vérité" ? », *op. cit.*, p. 132, pt 49.

139 En ce sens, voy. rapport préc., A/70/361, p. 19, § 37.

Dans son examen, la Cour rappelle que l'article 10, paragraphe 2, de la Convention ne tolère point de restrictions à la liberté d'expression dans le domaine du discours politique ou des questions d'intérêt général[140].

41. La protection des lanceurs d'alerte ne semble pouvoir être activée que si la violation de l'intérêt général atteint un seuil important de gravité[141]. La juridiction européenne souligne en effet que ladite protection ne s'applique qu'aux informations confidentielles ou secrètes « que les citoyens ont un *grand* intérêt à voir divulguer ou publier »[142].

À la faveur de l'affaire des « *Cambridge Analytica Files* », révélée grâce au concours de plusieurs lanceurs d'alerte[143], on rappellera que la notion d'intérêt général doit, d'après le Comité des ministres du Conseil de l'Europe, « pour le moins, inclure les violations de la loi et des droits de l'homme » (voy. *supra*, n° 8)[144]. En l'occurrence, il est manifeste que la collecte des « données *Facebook* » des personnes répondant au questionnaire psychologique proposé par *Global Science Research* (GSR) et leur partage avec la société Cambridge Analytica, ainsi que la récolte, au passage, des « données *Facebook* » des amis de la personne répondant au questionnaire[145] contreviennent aux règles les plus élémentaires prévues par le RGPD[146]. Entre autres, on signalera que les personnes qui ont répondu au questionnaire n'ont pas été informées de la collecte de leurs « données *Facebook* » (collecte directe). De même, les amis de ces personnes n'ont pas été informées du fait que leurs données avaient été partagées avec Cambridge Analytica (collecte indirecte). Par ailleurs, notons également que le recours par Cambridge Analytica aux « *dark posts* » dans le cadre de la campagne du président Trump, soit des sortes de messages promotionnels individualisés et éphémères[147], porte

140 Voy. not. Cour eur. D.H., *Görmüs*, préc., § 41 ; *Guja*, préc., § 74 ; *Heinisch*, préc., § 66.

141 J.-Ph. Foegle, « Le lanceur d'alerte dans l'Union européenne : démocratie, management, vulnérabilité(s) », *op. cit.*, p. 118. En ce sens, voy. aussi la proposition de directive précitée du 23 avril 2018 qui a pour objectif de détecter et de prévenir les préjudices *sérieux* (nous soulignons) à l'intérêt public (voy. not. considérants n^os^ 3 et 29).

142 Nous soulignons. Voy. not. Cour eur. D.H., *Guja*, préc., § 74 ; *Görmüs*, préc., § 50.

143 Ils seraient au nombre de trois. Voy. not. C. Cadwalladr, « Mark Gettleson : the Reluctant "Third Whistleblower" on Vote Leave Spending », 14 avril 2018, *The Guardian.com* (consulté le 15 avril 2018).

144 Recommandation CM/Rec (2014) 7, annexe, section I, principe 2.

145 Voy. not. P. Lewis et J. C. Wong, « Facebook Employs Psychologist Whose Firm Sold Data to Cambridge Analytica », 18 mars 2018, *The Guardian.com* (consulté le 15 avril 2018).

146 E. Wery, « Cambridge Analytica : comprendre le dossier en 5 minutes », 10 avril 2018, *Droit & Technologies.org* (consulté le 12 avril 2018).

147 Voy. not. P. Guyonnet, « Les patrons de Cambridge Analytica se félicitent d'avoir piloté "toute la campagne de Trump" », 21 mars 2018, *The Huffington Post.fr* ; H. Grassegger et M. Krogerus « The Data That Turned the World Upside Down », 28 janvier 2017, actualisé le 17 mars 2018, *Motherboard.vice.com* (consulté le 15 avril 2018).

atteinte à la liberté d'opinion des personnes qui ont été ciblées voir au principe même de la démocratie[148].

42. En tout état de cause, il est évidemment souhaitable que les États membres définissent ce que recouvre l'intérêt général aux fins de leur cadre national de protection des lanceurs d'alerte « […] de sorte que toute personne soit raisonnablement censée comprendre ce que l'intérêt général recouvre et ne recouvre pas, et soit en mesure de prendre une décision éclairée »[149].

iii. – *L'authenticité des informations divulguées*

43. En troisième lieu, la Cour européenne des droits de l'homme exige que l'information divulguée ou publiée soit authentique, c'est-à-dire supposée exacte et digne de crédit. La Cour laisse le soin aux États membres de sanctionner les dénonciations qui s'avèrent diffamatoires[150]. La Commission européenne, de son côté, les oblige à une telle sanction dans le but « de décourager les dénonciations malveillantes et abusives qui affectent l'effectivité et la crédibilité du système tout entier de protection des lanceurs d'alerte, ainsi que de prévenir les dommages injustifiés à la réputation des personnes concernées »[151].

44. La Cour de Strasbourg ne va pas jusqu'à exiger que les révélations soient *in fine* confirmées par les autorités qui s'en sont saisies[152]. Il suffit que les allégations du requérant ne soient pas « dépourvues de fondement factuel »[153]. À ce sujet, le rapporteur spécial à l'ONU, David Kaye, déconseille d'exiger une analyse poussée de la part du lanceur d'alerte[154]. Dans son appréciation, la Cour européenne garde, par ailleurs, à l'esprit le principe de présomption de bonne foi établi dans la résolution 1729(2010) de l'Assemblée parlementaire du Conseil de l'Europe[155].

148 Voy. not. « Facebook, l'envers du réseau », *Envoyé spécial*, 12 avril 2018, France 2.
149 Recommandation CM/Rec (2014) 7, exposé des motifs, § 44.
150 Cour eur. D.H., *Balenović* (déc.), préc.
151 Proposition de directive du 23 avril 2018, mémorandum explicatif, p. 13 et considérant n° 78.
152 Ainsi, une erreur d'appréciation commise de bonne foi ne doit pas faire perdre au lanceur d'alerte le bénéfice de la protection (en ce sens, voy. not. proposition de directive du 23 avril 2018, mémorandum explicatif, p. 12).
153 Cour eur. D.H., *Heinisch*, préc., § 79.
154 Rapport préc., A/70/361, p. 16, § 30.
155 Cour eur. D.H, *Bucur*, préc., § 107 ; *Heinisch*, préc., § 80. Selon ce principe, « tout donneur d'alerte doit être considéré comme agissant de bonne foi, sous réserve qu'il ait des motifs raisonnables de penser que l'information divulguée était vraie, même s'il s'avère par la suite que tel n'était pas le cas, et à condition qu'il n'ait pas d'objectifs illicites ou contraires à l'éthique » (résolution 1729(2010), préc., pt 6.2.4). Cette présomption a été reprise dans la proposition de directive du 23 avril 2018 (considérant n° 60).

45. L'examen du critère de l'authenticité conduit, de surcroît, la Cour de Strasbourg à tenir compte des devoirs et responsabilités que comporte l'exercice de la liberté d'expression. L'étendue de ces derniers dépend, d'un côté, de la situation du requérant et, de l'autre côté, du procédé technique utilisé[156].

S'agissant du premier critère, la Cour est attentive à la place occupée par le lanceur d'alerte dans la hiérarchie de son organisation, le secteur dans lequel il travaille et l'intensité du devoir de réserve auquel il est soumis[157]. À cet égard, il importe de rappeler l'affaire *Medzlis*, même si cette dernière ne concerne pas formellement des lanceurs d'alerte. Ainsi que nous l'avons déjà signalé, la Cour y a apprécié plus strictement les devoirs et responsabilités qui incombaient aux requérants au motif qu'il s'agissait d'ONG, et non de particuliers, et que ces ONG avaient rendu publiques leurs allégations, exerçant de la sorte « un rôle de chien de garde public semblable par son importance à celui de la presse »[158].

S'agissant du second critère, la Cour prend tout d'abord en considération la forme de diffusion (écrite, orale, …)[159]. L'affaire *Bathellier*, déjà évoquée, témoigne de la rigueur avec laquelle la Cour apprécie ce critère. Dans les faits, la juridiction a été attentive au fait que les dénonciations effectuées par le requérant incluaient des considérations personnelles et portaient sur des questions pour lesquelles plusieurs points de vue étaient possibles[160]. Cette appréciation a de quoi surprendre, voire inquiéter, dès lors que l'exercice de la liberté d'expression suppose, selon une jurisprudence constante, une certaine dose d'exagération[161]. Aussi, la Cour a souligné que le procédé de diffusion utilisé, qui reposait sur une lettre, soit un écrit, laissait au requérant la possibilité de mûrement réfléchir au contenu et au ton à employer dans ses allégations. Cet écrit devait être d'autant plus réfléchi qu'il était l'œuvre d'un employé occupant un poste de direction (voy. *supra*, premier critère).

Dans l'appréciation du second critère, la Cour tient également compte de la portée du moyen employé (revue locale ou nationale par exemple)[162]. La publication d'informations sur Internet, de par l'envergure de ses

156 Voy. not. Comm. eur. D.H., *Haseldine* (déc.) ; Cour eur. D.H., *Balenović* (déc.), préc.
157 Voy. not. Cour eur. D.H., *Bathellier* (déc.), préc. ; *Balenović* (déc.), préc.
158 Cour eur. D.H., *Medzlis*, préc., §§ 86 et 87.
159 Voy. not. Cour eur. D.H., *Bathellier* (déc.), préc.
160 Cour eur. D.H., *Bathellier* (déc.), préc.
161 En ce sens, voy. Q. Van Enis, « Une solide protection des sources journalistiques et des lanceurs d'alerte : une impérieuse nécessité à l'ère dite de la "post-vérité" ? », *op. cit.*, p. 136, pt 59 ; J.-Ph. Foegle, « Le lanceur d'alerte dans l'Union européenne : démocratie, management, vulnérabilité(s) », *op. cit.*, p. 113.
162 Voy. not. Cour eur. D.H., *Balenović* (déc.), préc.

effets, représente évidemment un procédé particulièrement attentatoire au regard du droit à la vie privée et à la protection de la réputation. Ainsi que nous l'avons vu, la révélation publique d'informations représente, en règle, l'ultime recours quoiqu'elle puisse s'imposer dans certaines circonstances exceptionnelles (voy. *supra*, n^os^ 38 et 39).

iv. – *Le préjudice causé à l'employeur*

46. La Cour de Strasbourg examine également l'ampleur et la gravité du préjudice causé à l'employeur par la divulgation d'informations.

Cet examen est cependant relativement formel dès l'instant où l'information divulguée a été jugée d'intérêt public par la Cour. Ainsi, si la Cour admet que des mesures de sanction prises à l'encontre d'un lanceur d'alerte peuvent avoir pour objectif de maintenir la confiance dans l'administration concernée[163] ou encore de « protéger le succès commercial et la viabilité des entreprises, pour le bénéfice des actionnaires et des employés, mais aussi pour le bien économique au sens large »[164], elle veille aussitôt[165] à rappeler que « l'intérêt général à la divulgation d'informations faisant état de pratiques discutables au sein d'une institution publique ou d'une entreprise est si important dans une société démocratique qu'il l'emporte sur l'intérêt qu'il y a à maintenir la confiance du public dans l'institution ou la réputation professionnelle de l'entreprise »[166]. Une libre discussion des problèmes d'intérêt public est en effet essentielle dans un État démocratique. C'est pourquoi il faut se garder de décourager les citoyens de se prononcer sur de tels problèmes[167].

v. – *La motivation du lanceur d'alerte*

47. Au-delà de la dimension objective de la bonne foi, appréciée à l'occasion du critère de l'authenticité des informations, la juridiction européenne tient encore compte de sa dimension subjective et, partant, de la motivation du salarié qui procède à la divulgation[168].

163 Cour eur. D.H., *Görmüs*, préc., § 63 ; *Bucur*, préc., § 115.
164 Cour eur. D.H., *Heinisch*, préc., §§ 89 et 90.
165 À tel point que Quentin Van Enis parle d'« autoneutralisation » (Q. VAN ENIS, « Une solide protection des sources journalistiques et des lanceurs d'alerte : une impérieuse nécessité à l'ère dite de la "post-vérité" ? », *op. cit.*, p. 140, pt 65).
166 Voy. not. Cour eur. D.H., 21 juillet 2011, req. n° 28274/08, *Heinisch*, § 90.
167 Voy. not. Cour eur. D.H. (ch.), 22 février 1989, req. n° 11508/85, *Barfod c. Danemark*, § 29 et *Bucur*, préc., § 115.
168 J.-Ph. FOEGLE, « Le lanceur d'alerte dans l'Union européenne : démocratie, management, vulnérabilité(s) », *op. cit.*, pp. 45-48.

Il est vrai que l'examen de la motivation permet, en droit[169] et dans le langage courant[170], de faire une distinction entre la « dénonciation » et la « délation ». Comme le relève le philosophe André Comte-Sponville, « ce n'est pas la dénonciation qui fait la délation, ce sont ses motivations – haine, appât du gain, amour propre. Quand Serge Klarsfeld dénonçait des criminels nazis réfugiés en Amérique du Sud, personne ne le traitait de délateur. Tout le monde voyait en lui un militant de la justice et de la mémoire »[171].

En ce sens, la Cour européenne des droits de l'homme veille à préciser qu'« un acte motivé par un grief ou une animosité personnels ou encore par la *perspective d'un avantage personnel, notamment un gain pécuniaire*, ne justifie pas un niveau de protection particulièrement élevé »[172]. Une telle appréciation peut se révéler problématique eu égard à la possibilité grandissante de récompenser les lanceurs d'alerte (voy. *supra*, n° 26). Il n'empêche que le lanceur d'alerte peut, de façon certaine, poursuivre concomitamment des intérêts plus personnels, telle que la volonté d'améliorer ses conditions de travail, à la condition de poursuivre, à titre principal, une finalité d'intérêt général[173].

48. En réalité, il faut dire que la pertinence du critère de la motivation est fortement discutée dans la littérature[174] dès lors que le lancement d'alerte tire sa justification, non pas de la vertu du lanceur d'alerte, mais bien de l'intérêt pour la société de la divulgation de l'information[175]. Le Comité des ministres du Conseil de l'Europe et le rapporteur spécial à l'ONU, David Kaye, se sont d'ailleurs prononcés en défaveur de ce critère[176]. Peu importe, souligne ce dernier, « la raison pour laquelle le lanceur d'alerte a fait ses révélations pourvu qu'elles soient véridiques »[177].

169 Voy. not. S. Brahy, « Dénonciation officielle et dénonciation civique », mercuriale prononcée le 1er septembre 1978 à l'audience solennelle de la cour d'appel de Liège, *Rev. dr. pén.*, 1978, p. 948 ; C. Guillain, « La dénonciation, comme source d'information à disposition des autorités judiciaires. La portée et les limites de la dénonciation en matière pénale », 6 janvier 2012, *Justice en ligne.be* (consulté le 6 septembre 2017).

170 Voy. not. *Dictionnaire Larousse en ligne*, disponible sur www.larousse.fr (consulté le 7 septembre 2017).

171 « La délation peut-elle être civique ? », regards croisés du philosophe A. Comte-Sponville et de l'avocat H. Leclerc, président honoraire de la Ligue des droits de l'homme, propos recueillis par A. Vidalie et publiés sur le site internet du journal *L'Express* le 4 avril 2005 (consulté le 29 mars 2017).

172 Nous soulignons. Voy. Cour eur. D.H., *Guja*, préc., § 77 ; *Heinisch*, préc., § 69 ; *Bucur*, préc., § 93 ; *Görmüs*, préc., § 50.

173 Voy. Cour eur. D.H., *Heinisch*, préc., § 83.

174 Voy. not. V. Junod, « La liberté d'expression du whistleblower. Cour européenne des droits de l'homme (Grande chambre), *Guja c. Moldova*, 12 février 2008 », *op. cit.*, p. 237 ; Q. Van Enis, « Une solide protection des sources journalistiques et des lanceurs d'alerte : une impérieuse nécessité à l'ère dite de la "post-vérité" ? », *op. cit.*, pp. 140 et 141 ; J.-Ph. Foegle, « Le lanceur d'alerte dans l'Union européenne : démocratie, management, vulnérabilité(s) », *op. cit.*, pp. 45-48.

175 J.-Ph. Foegle, « Le lanceur d'alerte dans l'Union européenne : démocratie, management, vulnérabilité(s) », *op. cit.*, p. 117.

176 Recommandation CM/Rec (2014) 7, annexe, section VII, principe 22 et rapport préc., A/70/361, p. 16, § 31.

177 Rapport préc., A/70/361, p. 16, § 31.

49. Sans doute l'enjeu principal repose-t-il sur la « conviction raisonnable »[178] du lanceur d'alerte dans le bien-fondé de son signalement au moment où il est effectué[179], ce que la Cour de Strasbourg vérifie d'ailleurs à deux reprises : lors de l'appréciation du critère de l'authenticité, d'une part, et lors de l'appréciation du critère de la motivation, d'autre part[180]. Partant, le lanceur d'alerte ne devrait pas perdre le bénéfice de sa protection du seul fait d'avoir commis de bonne foi une erreur d'appréciation des faits[181].

vi. – *La sévérité de la sanction encourue par le lanceur d'alerte*

50. Enfin, la Cour européenne des droits de l'homme apprécie la sévérité de la sanction encourue par le lanceur d'alerte. Dans cet examen, la Cour tient évidemment compte de la gravité de la sanction infligée concrètement au travailleur, mais aussi des répercussions de cette sanction sur sa carrière et sur son effet dissuasif à l'égard d'autres travailleurs de l'administration ou de l'entreprise visée, ainsi qu'à l'égard d'autres travailleurs, en cas de retentissement médiatique.

51. Dans les faits, la Cour de Strasbourg a jugé, sachant que les conditions de sa jurisprudence étaient toutes satisfaites, que le licenciement était une sanction particulièrement sévère puisqu'il s'agissait de la sanction la plus lourde qu'un employeur pouvait infliger[182]. En revanche, dans l'affaire *Bathellier*, dans laquelle les conditions n'étaient pas satisfaites pour les raisons exposées ci-dessus, la juridiction strasbourgeoise a jugé que le requérant n'avait « pas été puni de la sanction la plus lourde puisque finalement il a[vait] été licencié pour faute simple »[183].

3. – *La protection des sources journalistiques*

52. Ainsi que nous l'avons annoncé, le droit à la liberté d'expression garantit, au travers de la protection des sources, la confidentialité

178 Expression recommandée notamment dans P. STEPHENSON et M. LEVI, « La protection des "donneurs d'alerte" : rapport d'étude sur la faisabilité d'un instrument juridique sur la protection des employés qui divulguent des informations dans l'intérêt public », CDCJ (2012) 9 FIN, p. 31, pt 5.23 ; rapport préc., A/70/361, p. 16, § 30.

179 En ce sens, voy. proposition de directive du 23 avril 2018, art. 13.1 ; recommandation (2014) 7, annexe, section VII, principe 22.

180 Q. VAN ENIS, « Une solide protection des sources journalistiques et des lanceurs d'alerte : une impérieuse nécessité à l'ère dite de la "post-vérité" ? », *op. cit.*, p. 141, § 68.

181 Recommandation (2014) 7, annexe, section VII, principe 22 ; proposition de directive du 23 avril 2018, mémorandum explicatif, p. 12 et considérant n° 60. Voy. aussi rapport préc., A/70/361, p. 16, § 30.

182 Voy. not. Cour eur. D.H., *Guja*, préc., § 95 ; *Heinisch*, préc., § 91.

183 Cour eur. D.H., *Bathellier* (déc.), préc.

de l'identité des lanceurs d'alerte qui s'adressent à un journaliste en vue de mettre à la disposition du public un certain nombre d'informations (signalement public)[184]. En revanche, ladite protection ne vaut pas lorsque le lanceur d'alerte contacte un organe de gouvernance ou une autorité étatique en vue de prévenir ou de sanctionner une infraction (signalement interne et externe). La confidentialité de l'identité du lanceur d'alerte peut néanmoins être garantie sur la base d'autres fondements juridiques, à savoir le droit à la vie privée et à la protection des données, comme nous le verrons par la suite.

53. L'expression « journaliste » fait aujourd'hui l'objet d'une interprétation fonctionnelle[185]. Ainsi, le Conseil de l'Europe définit le terme « journaliste » comme « toute personne physique ou morale pratiquant à titre régulier ou professionnel la collecte et la diffusion d'informations au public par l'intermédiaire de tout moyen de communication de masse »[186].

Il résulte en effet de la mutation du paysage médiatique de ces dernières années, liée entre autres à la démocratisation d'Internet, que d'autres personnes que des journalistes professionnels jouent désormais le « rôle de chien de garde du public », selon l'expression consacrée par la Cour européenne des droits de l'homme, en ce qu'elles collectent des informations dans le but de les diffuser[187]. Aussi – et c'est là un deuxième critère important dans l'appréciation de la notion de source journalistique – il ne semble pas exclu qu'une relation de confiance semblable à celle qui unit un journaliste professionnel à sa source puisse s'établir ailleurs, par exemple entre un bloggeur et son informateur[188] ou entre les gestionnaires d'une plateforme de lancement d'alerte et ses lanceurs d'alerte[189]. À ce sujet, le Comité des ministres du Conseil de l'Europe précise d'ailleurs que la protection des sources devrait « s'étendre à

184 En ce sens, voy. not. Cour eur. D.H., *Görmüs*, préc., § 60 ; UNODC, *Resource Guide on Good Practices in the Protection of Reporting Persons*, *op. cit.*, pp. 16 et 17 ; D. Banisar, « Silencing Sources : An International Survey of Protections and Threats to Journalists' Sources », *Privacy International Global Survey Series*, 8 novembre 2007, p. 49 ; Q. Van Enis, « Une solide protection des sources journalistiques et des lanceurs d'alerte : une impérieuse nécessité à l'ère dite de la "post-vérité" ? », *op. cit.*, p. 99, § 4 ; D. Voorhoof, « Freedom of Journalistic Newsgathering, Access to Information, and Protection of Whistleblowers under Article 10 ECHR and the Standards of the Council of Europe », in *Comparative Perspectives on the Fundamental Freedom of Expression* (A. Koltay éd.), Budapest, Kluwer, 2015, p. 300.

185 Sur le sujet, voy. Q. Van Enis, *La liberté de la presse à l'ère numérique*, coll. du CRIDS, Bruxelles, Larcier, 2015, p. 649, n^os^ 509 et s.

186 Recommandation R (2000) 7 du Comité des ministres aux États membres sur le droit des journalistes de ne pas révéler leurs sources d'information, adoptée par le Comité des ministres le 8 mars 2000, lors de la 701^e^ réunion du Comité des ministres, annexe, définition a).

187 Rapport préc., A/70/361, p. 11. Voy. aussi D. Banisar, « Silencing Sources : An International Survey of Protections and Threats to Journalists' Sources », *op. cit.*, p. 31 ; Q. Van Enis, *La liberté de la presse à l'ère numérique*, *op. cit.*, p. 658, n° 512.

188 Q. Van Enis, *La liberté de la presse à l'ère numérique*, *op. cit.*, p. 625, n° 488 et p. 653, n° 511.

189 En ce sens, voy. recommandation CM/Rec (2011) 7, préc., pt 73.

l'identité des utilisateurs qui mettent à disposition des contenus d'intérêt public sur des espaces partagés en ligne conçus pour faciliter la communication de masse interactive (ou de groupe), y compris les plates-formes de partage de contenu et les services de réseaux sociaux »[190].

Partant, tous ces « communicateurs sociaux »[191] devraient pouvoir revendiquer le droit à la confidentialité de leurs sources[192].

54. Dans les faits, il n'est pas aisé de faire le départ entre les prestataires d'hébergement et les plateformes numériques exerçant une fonction journalistique[193]. La distinction est pourtant importante : le premier bénéficie, sous certaines conditions, d'une exemption de responsabilité, mais peut être tenu, en contrepartie, de collaborer avec les autorités étatiques[194] ; le second est, quant à lui, tenu d'assumer la responsabilité de ce qu'il divulgue mais bénéficie en amont de la protection de ses sources.

En tout état de cause, un même acteur ne pourrait bénéficier dans le même temps de l'exemption de responsabilité profitant aux hébergeurs et de la protection des sources journalistiques[195].

Quoique la question ne soit actuellement pas tranchée, il nous semble que les plateformes numériques de type « *WikiLeaks* » que l'on voit éclore dans la mouvance des lanceurs d'alerte doivent pouvoir bénéficier de la protection des sources dans la mesure où ces dernières incitent les tiers, par l'anonymat conféré, à leur confier des informations d'intérêt général dans l'optique d'une diffusion future au public[196]. En l'occurrence, l'anonymat fourni par la célèbre plateforme créée par Julian Assange repose sur le réseau TOR[197], le logiciel TAIL[198] et le financement via des monnaies cryptées telles que le Bitcoin[199]. D'autres

190 *Ibid.*

191 L'expression est employée par la Commission interaméricaine des droits de l'homme (« Déclaration de principes sur la liberté d'expression », principes 8 et 13).

192 Rapport préc., A/70/361, p. 11, § 18.

193 Sur le sujet, voy. not., dans le présent ouvrage, F. TRÉGUER, « Anonymat et chiffrement, composantes essentielles de la liberté de communication ». Voy. aussi Q. VAN ENIS, *La liberté de la presse à l'ère numérique*, *op. cit.*, pp. 656 et 657, n^os^ 512 et 513.

194 Art. 14 et 15 de la directive 2000/31/CE du Parlement européen et du Conseil du 8 juin 2000 relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (« directive sur le commerce électronique »), *J.O.U.E.*, L 178/1 à L 178/16, 17 juillet 2000.

195 Q. VAN ENIS, *La liberté de la presse à l'ère numérique*, *op. cit.*, p. 656, n° 512.

196 *Contra*, voy. B. VAN DER SLOOT, « WikiLeaks : te actief voor een webhoster, te passief voor een journalistiek medium », *NJB*, 25 mars 2011, pp. 734-739, cité par Q. VAN ENIS, *La liberté de la presse à l'ère numérique*, *op. cit.*, p. 657, note 2631.

197 Le nom dérive de l'acronyme du projet de logiciel d'origine, intitulé « *The Onion Router* ».

198 « *The Amnesic Incognito Live System* ».

199 Le financement de l'organisation *WikiLeaks* repose entièrement sur le public. Les donations peuvent se faire notamment via la monnaie virtuelle sécurisée et anonyme Bitcoin (« Donate to WikiLeaks », https://shop.wikileaks.org/donate, consulté le 13 avril 2018).

outils numériques se fondent désormais sur la même technologie. C'est le cas du site www.sourcesure.eu, le site d'envoi anonyme de documents confidentiels vers les médias[200], de la plateforme *EuLeaks*, lancée par les parlementaires européens du groupe Verts/ALE[201] ou encore de la plateforme *GlobaLeaks*, qui permet un lancement d'alerte anonyme et sûr et est utilisé par plus de 60 organismes partout dans le monde, lesquels incluent « des médias indépendants, des activistes, des organismes publics, des sociétés et plus encore »[202]. Cette dernière initiative doit toutefois être distinguée des autres initiatives en ce qu'elle se contente de fournir en libre accès une technologie sans offrir de service de diffusion[203]. Partant, une telle plateforme ne devrait pouvoir bénéficier de la protection des sources mais devrait se voir appliquer l'exemption de responsabilité reconnue aux hébergeurs.

55. S'agissant de la portée concrète de la protection des sources journalistiques, il découle de l'arrêt de principe rendu par la Cour européenne des droits de l'homme dans l'affaire *Goodwin* que le bénéficiaire de la protection a le droit de garder le silence sur ses sources d'information[204]. Cela signifie également que le bénéficiaire de la protection ne peut être contraint de collaborer à l'identification de ses sources, en communiquant par exemple des informations susceptibles d'aboutir à un tel résultat[205]. Du reste, le droit des journalistes de taire leurs sources interdit également de procéder à des perquisitions et saisies à leur domicile et au siège de leur rédaction, dès l'instant où de telles mesures viseraient en réalité à contourner la protection des sources[206].

La protection des sources journalistiques témoigne donc d'une reconnaissance indirecte de l'anonymat et de la confidentialité des communications par la Cour de Strasbourg[207].

200 Consulté le 10 juin 2017.

201 Disponible à l'adresse www.greens-efa.eu/ (consulté le 10 juin 2017).

202 https://www.globaleaks.org/fr/, page d'accueil (consulté le 25 février 2018). Voy. par exemple, *PubLeaks*, *WildLeaks* et *MafiaLeaks*.

203 Hermes Center, « Projects & Technologies –GlobaLeaks –What GlobaLeaks is not », *Hermes Center*, https://www.hermescenter.org/home/projects-technologies/globaleaks/(consulté le 14 avril 2018).

204 Cour eur. D.H., préc., § 39.

205 Cour eur. D.H. (4e sect.), 15 décembre 2009, req. n° 821/03, *Financial Times et autres c. Royaume-Uni*, § 70.

206 Voy. not. Cour eur. D.H. (4e sect.), 25 février 2003, req. n° 51772/99, *Roemen et Schmit c. Luxembourg*, § 57 ; Cour eur. D.H. (2e sect.), 15 juillet 2003, req. n° 33400/96, *Ernst et autres c. Belgique*, § 103 ; Cour eur. D.H. (2e sect.), 27 novembre 2007, req. n° 20477/05, *Tillack c. Belgique*, § 65. En ce sens, voy. aussi recommandation R (2000) 7, préc., annexe, principe 6(a) ; Q. Van Enis, *La liberté de la presse à l'ère numérique*, *op. cit.*, p. 671, n° 520.

207 Voy., dans le présent ouvrage, F. Tréguer, « Anonymat et chiffrement, composantes essentielles de la liberté de communication ».

À la lumière de ces considérations, on peut s'interroger sur les risques que suscitent l'achat de données par l'État à un journaliste. En fonction des paramètres de sécurité adoptés par le journaliste, il ne semble pas exclu que les métadonnées attachées aux données vendues puissent permettre à l'État d'identifier la source d'information et, de la sorte, contourner le droit à la protection des sources.

56. Il n'empêche que la protection des sources peut être levée dans des circonstances exceptionnelles strictement limitées par la loi et conformes à l'article 10, paragraphe 2, de la CEDH[208].

S'agissant des plateformes de lancement d'alerte, cela signifie que leurs gestionnaires devraient être, le cas échéant, techniquement capables d'identifier leurs utilisateurs, ce qui ne semble actuellement pas le cas[209]. De fait, une telle possibilité risquerait d'affaiblir la nécessaire confiance qui doit unir le gestionnaire d'une plateforme de lancement d'alerte à ses utilisateurs.

Au demeurant, le lanceur d'alerte demeure responsable de ses actes conformément au droit de chaque État membre. Si la protection des sources empêche, en règle, les autorités de passer par le journaliste pour identifier la source d'information, rien n'empêche en effet ces dernières de prendre des mesures d'informations ou d'instruction en vue d'aboutir à cette identification[210].

B. – *La protection du lanceur d'alerte sous l'angle du droit à la vie privée*

57. Comme tout citoyen, le lanceur d'alerte jouit du droit au respect de la vie privée[211]. Celui-ci est consacré, en Europe, par l'article 8 de la Convention européenne des droits de l'homme et par l'article 7 de

208 Voy. not. Cour eur. D.H., *Goodwin*, préc., § 39 ; recommandation R (2000) 7, préc., annexe, principe 3 ; rapport préc., A/70/361, p. 13, § 22.

209 Le système d'exploitation « *Tails* », utilisé par les actuelles plateformes de lancement d'alerte, serait « amnésifère » en ce qu'il permettrait à l'ordinateur du lanceur d'alerte de fonctionner sans ne rien garder en mémoire (Y. EUDES, « Hermès, les messagers de l'Internet libre », 17 octobre 2014, *Le Monde*, https://www.lemonde.fr/pixels/article/2014/10/17/hermes-les-messagers-de-l-internet-libre_4508097_4408996.html [consulté le 26 février 2018]).

210 Par exemple, la Cour de cassation belge a jugé, dans un arrêt du 6 février 2008, que le dispositif légal belge, qui constitue, à dire vrai, un modèle en Europe, « se borne à interdire d'user de la voie du journaliste pour remonter à la source de l'information, la loi ne prohibant pas, en revanche, les mesures d'information ou d'instruction directement dirigées vers l'identification d'une personne suspectée d'avoir violé une obligation légale de secret en dévoilant des informations à un journaliste » (Q. VAN ENIS, *La liberté de la presse à l'ère numérique*, *op. cit.*, p. 107, n° 17).

211 En ce sens, voy. le « Corporate Whistleblower's Bill of Rights and Responsabilities », dans T. DEVINE et T. F. MAASSARANI, *The Corporate Whistleblower's Survival Guide : a Handbook for Committing the Truth*, *op. cit.*, pp. 201 et 202.

la Charte des droits fondamentaux de l'Union européenne. Eu égard au sujet qui nous occupe, il convient d'attirer l'attention sur le fait que le droit à la vie privée couvre notamment le droit au secret des communications (1).

Comme nous l'avons déjà signalé, c'est à l'occasion de l'implémentation du « *SOX Act* » par des entreprises européennes que s'est posée, pour la première fois, la question de la compatibilité du *whistleblowing* américain avec le droit de l'UE et, en l'occurrence, avec la règlementation relative à la protection des données (2). Si le droit à la protection des données à caractère personnel est étroitement lié au droit à la vie privée, il a progressivement acquis au sein de l'Union une autonomie par rapport à ce dernier[212].

1. – *Le droit au secret des communications électroniques*

58. La notion de « correspondance » se voit conférer une interprétation large par la Cour européenne des droits de l'homme. C'est pourquoi la doctrine parle volontiers d'un « droit à la communication » pour désigner ce droit[213]. Par « correspondance », la Cour de Strasbourg entend toute communication privée, qu'elle relève de la vie « privée » ou « professionnelle »[214], et quelle qu'en soit la forme : téléphonique[215], papier[216], électronique[217] ou autre[218], l'objectif étant d'en protéger la confidentialité[219]. Il s'ensuit qu'est protégé tant « le droit à communiquer que le contenu »[220].

À cet égard, on soulignera que la protection des personnes physiques à l'égard de la confidentialité des communications électroniques et du traitement de ces communications fait l'objet d'un texte exprès en

[212] Ainsi, la Charte des droits fondamentaux de l'Union européenne consacre distinctement le droit à la protection des données à caractère personnel (art. 8) du droit au respect de la vie privée (art. 7). Sur l'autonomie du droit à la protection des données au sein de l'Union européenne, voy. not. C. DE TERWANGNE, K. ROSIER et B. LOSDYCK, « Lignes de force du nouveau Règlement relatif à la protection des données à caractère personnel », *R.D.T.I.*, 2016, n° 62, pp. 6 et 7, n° 3.

[213] Voy. not. P. DE HERT, « Het recht op privacy », in *Handboek EVRM*, Deel II, *Artikelsgewijze commentaar* (J. VANDE LANOTTE et Y. HAECK éd.), Anvers, Intersentia, 2005, p. 710.

[214] Voy. not. Cour eur. D.H., 16 décembre 1992, req. n° 13710/88, *Niemietz c. Allemagne*, § 32.

[215] Voy. not. Cour eur. D.H. (ch.), 24 avril 1990, req. n° 11105/84, *Huvig c. France*, §§ 8 et 25 ; Cour eur. D.H. (4e sect.), 18 mai 2010, req. n° 26839/05, *Kennedy c. Royaume-Uni*, § 118.

[216] Cour eur. D.H., *Niemietz*, préc., § 32.

[217] Voy. not. Cour eur. D.H. (4e sect.), 27 septembre 2005, req. n° 50882/99, *Petri Sallinen e.a. c. Finlande*, § 71 ; Cour eur. D.H., *Kennedy*, préc., § 118.

[218] Voy. not. Cour eur. D.H. (5e sect.), 6 décembre 2012, req. n° 12323/11, *Michaud c. France*, § 90.

[219] Voy. not. Cour eur. D.H. (2e sect.), 12 juin 2007, req. n° 70204/01, *Frérot c. France*, § 53 ; Cour eur. D.H., *Michaud*, préc., § 90.

[220] S. DE RAEDT, « La portée du droit au respect de la vie privée et le droit de visite de l'administration fiscale – L'importance de l'arrêt Bernh Larsen nuancée », *R.G.C.F.*, 2015/3, p. 158.

Europe : la directive « *e-privacy* »[221]. C'est dire combien la confidentialité des communications – qu'il s'agisse du contenu ou des métadonnées qui les accompagnent – est centrale en Europe.

59. Quoique la Cour européenne des droits de l'homme ne se soit jamais formellement prononcée sur la violation supposée du droit à la vie privée d'un lanceur d'alerte, il ne fait pas de doutes que l'interception secrète d'e-mails et/ou la copie d'e-mails stockés sur l'ordinateur d'un lanceur d'alerte pourrait constituer une ingérence dans son droit au respect de la correspondance[222].

60. Enfin, soulignons que la Cour de Strasbourg accorde une protection renforcée aux échanges entre les avocats et leurs clients, qu'il s'agisse d'échanges téléphoniques[223] ou de données électroniques[224]. La Cour de Luxembourg reconnaît également, de longue date, la confidentialité du courrier entre une personne poursuivie et son avocat[225]. Cela se justifie par le fait que les avocats se voient confier une mission fondamentale dans une société démocratique : la défense des justiciables[226].

2. – *Le droit à la protection des données à caractère personnel*

61. Dès l'instant où le fonctionnement d'un dispositif d'alerte repose sur la collecte et l'exploitation de données à caractère personnel, les règles européennes relatives à la protection des données doivent être respectées[227]. Ceci est quasi toujours le cas dès lors que la gestion des signalements passe, à l'ère numérique, nécessairement par un outil informatique de traitement automatisé.

221 Directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive « Vie privée et communications électroniques »), *J.O.U.E.*, L 201/37 à L 201/47, 31 juillet 2002.

222 Sur la protection de la confidentialité des communications à l'aune des droits à la vie privée et à la liberté d'expression, voy. not. rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, Frank La Rue, sur les effets de la surveillance des communications par les États sur l'exercice des droits à la vie privée et à la liberté d'opinion et d'expression, A/HRC/23/40, 17 avril 2013.

223 Voy. not. Cour eur. D.H. (plén.), 6 septembre 1978, req. n° 5029/71, *Klass e.a. c. Allemagne*, § 41 ; Cour eur. D.H. (ch.), 25 mars 1998, req. n° 13/1997/797/1000, *Kopp c. Suisse*, § 50.

224 Voy. not Cour eur. D.H. (4e sect.), 1er juillet 2008, req. n° 74336/01, *Wieser et Bicos Beteiligungen c. Autriche*, § 45.

225 CJCE, 18 mai 1982, aff. 155/79, *AM & S. Europe Limited*, *Rec.*, 1982, p. 1575, cité dans R. ERGEC, *Protection européenne et internationale des droits de l'homme*, 3e éd., Bruxelles, Larcier, 2014, p. 123.

226 Voy. not. Cour eur. D.H. (5e sect.), 21 janvier 2010, req. n° 43757/05, *Xavier Da Silveira c. France*, § 36 ; Cour eur. D.H., *Michaud*, préc., § 118 ; Cour eur. D.H. (5e sect.), 24 juillet 2008, req. n° 18603/03, *André et autres c. France*, § 41.

227 Proposition de directive du 23 avril 2018, art. 18 et considérants nos 55 et 58. G29, avis 1/2006 relatif à l'application des règles de l'UE en matière de protection des données aux mécanismes internes de dénonciation des dysfonctionnements dans les domaines de la comptabilité, des contrôles comptables internes, de l'audit, de la lutte contre la corruption et la criminalité bancaire et financière, p. 6.

L'encadrement juridique des dispositifs d'alerte, notamment au regard du droit à la vie privée et à la protection des données, représente un enjeu majeur tant pour éviter les alertes injustifiées que pour encourager les alertes justifiées[228]. Le respect de la protection des données est également susceptible de renforcer les dispositifs d'alerte en raison des garanties que cette protection comporte en termes de confidentialité, de transparence et de sécurité notamment[229].

62. La protection des données à caractère personnel repose, en droit de l'UE, sur trois textes : le Règlement général de protection des données, la directive « Police & Justice »[230] et la directive « *e-privacy* ». Ces trois textes sont susceptibles de s'appliquer au lancement d'alerte. Vu le thème qui nous occupe, précisons qu'il appartient aux États membres, conformément à l'article 85 du RGPD, de concilier, par la loi, le droit à la protection des données à caractère personnel et le droit à la liberté d'expression et d'information[231]. La directive « *e-privacy* » est, quant à elle, susceptible de s'appliquer aux trois types de signalement en ce qu'elle complète la directive « vie privée », que le RGPD a vocation à remplacer, dans le domaine des communications électroniques[232]. Mentionnons que la directive « *e-privacy* » sera prochainement remplacée par un règlement en vue d'assurer la cohérence de ses règles avec le RGPD[233].

La compatibilité de la mise en place de dispositifs de signalement interne avec la protection des données a donné lieu à un examen approfondi de la part du Groupe de l'article 29 et du Contrôleur européen de la protection des données (ci-après : « CEPD »). Les orientations données dans ce cadre devraient, *mutatis mutandis*, s'appliquer au signalement externe et au signalement public[234]. Dans le cadre du présent chapitre,

228 Voy. not. CPVP, recommandation n° 01/2006, p. 2.

229 En ce sens, voy. not. CEPD, Lignes directrices relatives au traitement d'informations à caractère personnel dans le cadre d'une procédure d'alerte éthique, 18 juillet 2016 (ci-après : « Lignes directrices du 18 juillet 2016 »), p. 4, pt 3 ; G29, avis n° 1/2006, p. 20.

230 Directive 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil, *J.O.U.E.*, L 119/89 à L 119/131, 4 mai 2016.

231 Sur le sujet, voy. Q. Van Enis, « La conciliation entre le droit à la liberté d'expression et le droit à la protection des données à caractère personnel dans le RGPD », in *Le Règlement général sur la protection des données (RGPD/GDPR)* (C. de Terwangne et K. Rosier éds), Bruxelles, Larcier, 2018, pp. 757-789.

232 Art. 1.1 de la directive « *e-privacy* ».

233 Proposition de règlement du Parlement européen et du Conseil concernant le respect de la vie privée et la protection des données à caractère personnel dans les communications électroniques et abrogeant la directive 2002/58/CE (règlement « Vie privée et communications électroniques »), 10 janvier 2017, COM(2017) 10 final.

234 En ce sens, la CPVP a ainsi choisi de ne pas s'exprimer sur la conformité au RGPD du dispositif de *whistleblowing* imposé par la loi du 18 septembre 2017, estimant manifestement – la CPVP ne l'indique pas explicitement – que les orientations qu'elle avait fournies en 2006 suffisaient. Or, la loi du 18 septembre

focalisons-nous sur les droits dont jouit le lanceur d'alerte en vertu de la protection des données ainsi que sur les mesures de sécurité qui doivent être prises par le responsable du traitement. Pour le surplus, nous renvoyons à d'autres études plus spécialisées[235].

63. Toutes les parties intervenantes, à savoir le lanceur d'alerte, la personne mise en cause et les tiers éventuels – tels que des collègues témoins des faits dénoncés – jouissent, en règle, des « droits de la personne concernée » prévus au chapitre III du RGPD. Ces droits comprennent le droit d'information, le droit d'accès, le droit d'opposition, le droit de rectification et le droit à l'effacement[236]. Comme à l'époque de la directive « vie privée », ils peuvent comporter des dérogations afin de concilier les droits, libertés et intérêts des parties en présence.

Eu égard au sujet qui nous occupe, il importe de souligner que le droit d'accès ne peut permettre d'accéder aux données personnelles d'autrui, sauf si celui-ci a donné son accord exprès[237]. Ainsi, le lanceur d'alerte ne peut accéder, sauf accord de leur part, aux données à caractère personnel de la personne mise en cause et des tiers éventuels. À l'inverse, la personne mise en cause ne peut pas davantage connaître l'identité du dénonciateur ou celle des tiers impliqués, ni leurs données personnelles, sauf en cas d'accord de leur part.

L'interdiction de divulguer l'identité des parties impliquées doit toutefois pouvoir être levée en cas d'allégations fausses ou abusives, qu'elles soient imputables au lanceur d'alerte, à la personne mise en cause ou à des tiers[238]. La décision de levée devrait être prise après consultation du délégué à la protection des données, le cas échéant[239]. Il s'ensuit que le logiciel de traitement utilisé par l'entreprise ou l'administration

2017 transpose, en droit belge, la quatrième directive anti-blanchiment, laquelle établit à la fois un dispositif de signalement interne et un dispositif de signalement externe.

235 Voy. not. O. GOFFARD, « Les systèmes d'alerte professionnelle (*whistleblowing*) et le respect de la vie privée : du Sarbanes-Oxley Act à la recommandation de la Commission de la vie privée », *T.B.H.*, 2007/3, pp. 201-220 ; K. ROSIER, « Chapitre III : Hypothèses dans lesquelles une violation des obligations de secret ou de confidentialité pourrait être admise, Section 1. *Whistleblowing* », *op. cit.*, pp. 129-150 ; F. COTON et J.-Fr. HENROTTE, « Le lanceur d'alerte : une personne concernée par le traitement de ses données à caractère personnel, mais également par son avenir professionnel… », *op. cit.*, pp. 43-78 ; C. KUNER, *European Data Protection Law. Corporate Compliance and Regulation*, *op. cit.*, pp. 270-277 ; A. LACHAPELLE, « Le lancement d'alerte (*whistleblowing*) à l'ère du Règlement Général de Protection des Données », in *Le Règlement général sur la protection des données (RGPD/GDPR)* (C. DE TERWANGNE et K. ROSIER éds), *op. cit.*, pp. 791-830.

236 Sur ce sujet, voy. not. Th. TOMBAL, « Les droits de la personne concernée dans le RGPD », in *Le Règlement général sur la protection des données (RGPD/GDPR)* (C. DE TERWANGNE et K. ROSIER éds), *op. cit.*, pp. 407-555.

237 Voy. not. G29, avis n° 1/2006, p. 15 ; CEPD, Lignes directrices du 18 juillet 2016, pp. 6 et 7.

238 CEPD, Opinion on a notification for Prior Checking regarding the European Ombudsman's Whistleblowing Procedure (Case 2014-0828), 4 décembre 2014, p. 5.

239 CEPD, Decision on internal rules concerning whistleblowing, 14 décembre 2015, art. 8. Voy. à cet égard l'art. 38.1 du RGPD.

devrait permettre, dans une telle hypothèse, de remonter à l'auteur de la dénonciation.

Au demeurant, précisons que l'autorité belge de protection des données a tiré de la protection des données le droit du lanceur d'alerte de savoir ce qu'il advient de son signalement ainsi que les suites qui y sont données[240]. La reconnaissance d'un tel droit tend à éviter, selon l'autorité belge, « que l'auteur de la dénonciation n'ait le sentiment (subjectif) que celle-ci n'est pas prise au sérieux et que pour cette raison, il transgresse intentionnellement la confidentialité de sa propre dénonciation, ce qui aura pour conséquence de violer la vie privée des personnes dénoncées et des tiers éventuels »[241]. Déçu du traitement de son signalement, le dénonciateur pourrait, en effet, être tenté de le porter en dehors de l'organisation, et notamment dans les médias. Pour les mêmes raisons, la Commission européenne consacre, dans sa proposition de directive du 23 avril dernier, l'obligation de tenir informé le lanceur d'alerte du suivi apporté à son signalement[242].

64. La confidentialité de l'identité du lanceur d'alerte et de son signalement constitue une garantie majeure au sein du système de protection élaboré tant par les autorités européennes de protection des données[243] que par les autres instances européennes[244] et internationales[245]. Le système d'alerte ne saurait en effet être efficace si le lanceur d'alerte craignait de voir révélés à des tiers son identité ainsi que le contenu de son signalement.

S'agissant, d'une part, de la confidentialité de l'identité du lanceur d'alerte, il importe concrètement que le dispositif d'alerte prévoit formellement l'interdiction de divulguer l'identité du lanceur d'alerte, ainsi que des éléments qui peuvent permettre son identification, pendant toute la durée du traitement de la dénonciation. Cette interdiction devrait néanmoins être levée si le lanceur d'alerte donne son accord, si

240 CPVP, recommandation n° 01/2006, p. 6. En faveur de la reconnaissance d'un droit de suivi au lanceur d'alerte, voy. aussi résolution du Parlement européen du 24 octobre 2017, préc., pt 32 ; T. Devine et T. F. Maassarani, *The Corporate Whistleblower's Survival Guide : a Handbook for Committing the Truth*, *op. cit.*, p. 202.

241 CPVP, recommandation n° 01/2006, p. 6.

242 Proposition de directive du 23 avril 2018, art. 5.1, d) (signalement interne), 6.2, b), 6.3 et 9.1, b) (signalement externe). Voy. aussi considérant n° 46 (signalement interne) et considérants n^{os} 49 et 50 (signalement externe).

243 Voy. not. G29, avis n° 1/2006, pp. 12 et 15.

244 Voy. not. proposition de directive du 23 avril 2018, considérants n^{os} 44, 48 et 55 et art. 5.1, 6.2 et 9 ; résolution du Parlement européen du 14 février 2017, préc., pt 15 ; Groupe des Verts/ALE du Parlement européen, Whistleblower protection in the public and private sector in the European Union. Draft directive, préc., art. 16 ; recommandation CM/Rec (2014) 7, annexe, section V, principe 18.

245 Rapport préc., A/70/361, p. 20, § 39 ; OECD, *CleanGovBiz – Integrity in practice : Whistle-blower protection : encouraging reporting*, juillet 2012, p. 13.

les investigations ne peuvent être poursuivies sans révéler son identité (par exemple s'il représente un témoin clé en justice)[246] ou, ainsi que nous venons de le voir, si le lanceur d'alerte s'est rendu coupable d'une dénonciation abusive.

Une distinction s'impose entre le régime de la confidentialité et celui de l'anonymat. Si dans les deux cas, l'identité du lanceur d'alerte ne peut être révélée, sauf consentement ou obligation légale, elle n'est connue de son destinataire que dans le premier cas[247].

Selon une opinion largement partagée, le signalement confidentiel devrait être préféré au signalement anonyme[248]. Une telle position s'explique par l'incompatibilité apparente du signalement anonyme avec le principe de loyauté[249]. Au-delà de la protection des données, d'autres raisons conduisent les autorités européennes à adopter cette position. L'identification du lanceur d'alerte paraît, en effet, nécessaire en vue d'assurer sa protection contre les représailles. Il peut être aussi utile aux autorités chargées du suivi de pouvoir contacter le lanceur d'alerte pour de plus amples renseignements. Il arrive, par ailleurs, que l'anonymat soit dans les faits impossible dans la mesure où les informations dénoncées ne sont connues que par un cercle réduit d'initiés. Du reste, on craint que l'anonymat n'encourage les dénonciations abusives et/ou malhonnêtes. Enfin, on redoute que l'anonymat ne renforce les suspicions mutuelles qui peuvent naître d'un dispositif d'alerte professionnelle et briser de la sorte la nécessaire confiance devant régner au sein d'une organisation.

En pratique, le recours à l'anonymat s'avère cependant indispensable dans certaines circonstances exceptionnelles, notamment pour des raisons liées à la psychologie du lanceur d'alerte[250] ou lorsque la dénonciation n'est pas organisée[251]. Des tiers intervenants à la procédure d'alerte, en qualité de témoins (par exemple, des collègues), pourraient en outre souhaiter bénéficier de l'anonymat[252]. L'utilisation courante d'une pla-

246 CEPD, Decision on internal rules concerning whistleblowing, préc., art. 8.

247 Voy. not. rapport préc., A/70/361, p. 20, § 40.

248 G29, avis n° 1/2006, p. 11 ; CEPD, Lignes directrices du 18 juillet 2016, p. 6, pt 12. Voy. aussi, au-delà du cadre de la protection des données : P. STEPHENSON et M. LEVI, « La protection des "donneurs d'alerte" : rapport d'étude sur la faisabilité d'un instrument juridique sur la protection des employés qui divulguent des informations dans l'intérêt public », *op. cit.*, p. 32 ; recommandation CM/Rec (2014) 7, section V, principe 18 et exposé des motifs, § 12 ; rapport préc., A/70/361, p. 20, § 40.

249 G29, avis n° 1/2006, p. 11.

250 On observe, par exemple, que la mise en place d'un dispositif ICT de surveillance sur le travail peut saper la volonté des employés de dénoncer des pratiques illégales ou irrégulières, sauf à leur accorder l'anonymat (G29, opinion 2/2017 on 8 June 2017 on data processing at work, WP 249, p. 10).

251 G29, avis n° 1/2006, p. 12.

252 Sur le témoignage anonyme, voy. not. Ch. DE VALKENEER, *Manuel de l'enquête pénale*, Bruxelles, Larcier/Politeia, 2005, pp. 91 et 92.

teforme en ligne amène par ailleurs à tolérer l'anonymat dès lors que ce dernier est perçu comme un outil fondamental de sécurisation des activités en ligne (voy. *infra*, n° 67).

S'agissant, d'autre part, de la confidentialité du signalement, on indiquera que la personne qui met en place un dispositif d'alerte (« responsable du traitement ») ou, le cas échéant, gère, un tel dispositif (« sous-traitant »)[253] est tenue, en application du RGPD, de traiter les données à caractère personnel « de façon à garantir une sécurité appropriée des données à caractère personnel […] à l'aide de mesures techniques ou organisationnelles appropriées »[254], telles que la pseudonymisation et le chiffrement des données[255]. Sans nul doute est-il utile de mutualiser la recherche et le développement de mesures techniques appropriées et de permettre leur déploiement. À ce sujet, on signalera que la technologie *GlobaLeaks*, développée par le Centre Hermes pour la transparence et les droits numériques de la personne, est libre d'utilisation[256]. D'où la référence mythologique au dieu « Hermès » qui tend à faire d'Internet un messager libre.

C. – *À la croisée du droit à la vie privée et à la liberté d'expression : le droit au chiffrement et à l'anonymat du lanceur d'alerte*

65. Véritable rempart contre les représailles dont un lanceur d'alerte peut pâtir, le droit à la confidentialité de l'identité du lanceur d'alerte est sans cesse souligné par les instances politiques. Ainsi que nous l'avons vu dans le présent chapitre, la protection des données et, dans une moindre mesure, la protection des sources, permettent de protéger la confidentialité de l'identité du lanceur d'alerte. La confidentialité est préférée à l'anonymat pour un certain nombre de raisons que nous avons exposées. Aussi, et surtout, les effets délétères de la dénonciation anonyme sont malheureusement bien connus, et ce depuis l'époque des sycophantes[257]. Son instrumentalisation durant la seconde guerre mon-

253 Cette dernière hypothèse vise la situation de l'entreprise qui externalise la gestion de ses alertes vers une entreprise spécialisée.

254 Art. 5.1, f), du RGPD.

255 CEPD, Lignes directrices du 18 juillet 2016, p. 12.

256 Hermes Center, « Projects & Technologies/OpenWhistleblowing », https://www.hermescenter.org (consulté le 14 avril 2018).

257 Sur le rapprochement entre la figure du lanceur d'alerte et celle du sycophante de la Grèce Antique, voy. P. Adam, « Le retour des sycophantes ? (à propos du whistleblowing) », *Droit ouvrier*, 2006, n° 695, pp. 281-296 ; N. Warembourg, « Le sycophante, un lanceur d'alerte ? Remarques historiques sur la délation et le délateur dans l'Athènes démocratique », in *Les lanceurs d'alerte. Quelle protection juridique ? Quelles limites ?* (M. Disant et D. Pollet-Panoussis dir.), Issy-les-Moulineaux, Lextenso, 2017, pp. 53-70.

diale par le gouvernement nazi et celui de Vichy nous a encore rappelé ses incommensurables dangers.

66. Pourtant, force est de constater que l'anonymat est parfaitement autorisé en pratique. En l'absence d'un cadre juridique protecteur complet et effectif, la confidentialité s'avère largement insuffisante. L'anonymat permet, d'une certaine façon, de palier à l'insuffisance actuelle du cadre légal. Aussi, le signalement anonyme présente l'avantage de se focaliser sur le contenu du signalement, sur son exactitude et sa fiabilité, plutôt que sur son auteur et ses qualités professionnelles et morales[258].

Ainsi, nous avons vu que des plateformes en ligne permettaient aux lanceurs d'alerte d'effectuer des signalements anonymes (voy. *supra*, n° 54). D'autre part, on observe que le signalement externe auprès des autorités publiques peut, en général, se faire de façon anonyme. La Commission européenne a ainsi lancé tout récemment un nouvel outil de lancement d'alerte anonyme en matière de pratiques anticoncurrentielles[259]. En outre, on soulignera qu'il est possible de communiquer de façon anonyme à l'Office européen de lutte antifraude (OLAF) des informations susceptibles d'être utiles pour la lutte contre la fraude, la corruption et toute autre activité illégale portant préjudice aux intérêts financiers de l'Union européenne[260].

67. En réalité, il apparaît que l'anonymat transpose, en ligne, les exigences de confidentialité attachées traditionnellement au lancement d'alerte. Le chiffrement ne protège en effet que le contenu des communications. Or, les métadonnées qui accompagnent ces communications permettent d'identifier l'auteur du signalement, notamment via son adresse IP. L'anonymat apparaît dans ce cadre comme le seul moyen de protéger l'identité du lanceur d'alerte[261].

Au-delà de la problématique du lancement d'alerte, un consensus se dégage aujourd'hui sur la nécessité de promouvoir et de protéger largement le chiffrement et l'anonymat comme des outils fondamentaux

258 En ce sens, voy. J. NEAR et M. MICELI, « Effective-Whistle Blowing », *Academy of management review*, 1995, vol. 20/3, p. 692 et 693 ; J.-Ph. FOEGLE, « Les lanceurs d'alerte. Étude comparée France – États-Unis », *op. cit.*, p. 84 ; rapport préc., A/70/361, p. 20, § 40.

259 « Anonymous Whistleblower Tool », http://ec.europa.eu/competition/cartels/whistleblower/index.html (consulté le 21 avril 2018).

260 « Fraud Notification System », https://ec.europa.eu/anti-fraud/olaf-and-you/report-fraud_en (consulté le 22 février 2018).

261 Sur le sujet, voy. not., dans le présent ouvrage, F. TRÉGUER, « Anonymat et chiffrement, composantes essentielles de la liberté de communication ».

de sécurisation des activités en ligne[262]. Au croisement du droit à la vie privée et du droit à la liberté d'opinion et d'expression[263], le chiffrement et l'anonymat garantissent aux personnes et aux groupes, pour reprendre les mots du rapporteur spécial David Kaye « un espace de confidentialité en ligne qui leur permet d'exercer leur liberté d'opinion et d'expression et les protège contre toute immixtion arbitraire ou illégale et contre toute attaque »[264]. Partant, les restrictions au chiffrement et à l'anonymat doivent respecter le triptyque fondamental établi par le second paragraphe des articles 8 et 10 de la CEDH : légalité-légitimité-proportionnalité[265].

V. Conclusion

68. L'affaire *Snowden*[266] et l'affaire *LuxLeaks*[267] ont illustré à suffisance, de par les modifications législatives qu'elles ont provoquées, les avantages que peut présenter le lancement d'alerte dans une société démocratique en termes de responsabilité, de transparence et de préservation de l'État de droit.

69. En toute hypothèse, le lanceur d'alerte est un citoyen. Il jouit donc de la protection des droits de l'homme. Cette protection repose, en particulier, sur le droit à la liberté d'expression et le droit au respect de la vie privée. Si le cadre juridique actuel, tel qu'interprété et appliqué par la Cour européenne des droits de l'homme et les autorités

262 Voy. spéc. rapport du rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression, David Kaye, sur l'usage du chiffrement et de l'anonymat dans l'exercice des droits à la liberté d'opinion et d'expression à l'ère numérique, A/HRC/29/32, 22 mai 2015, présenté au Conseil des droits de l'homme le 17 juin 2015 ; déclaration commune de la société civile soumise à la 29e session du Conseil des droits de l'homme des Nations unies : « Assurer la promotion des outils de chiffrement et d'anonymisation en ligne à l'ère numérique », https://rsf.org (consulté le 10 avril 2018). Voy. aussi déclaration commune de la Commission de réflexion et de propositions sur le droit et les libertés à l'âge numérique de l'Assemblée nationale française et la Commission sur les droits et devoirs sur Internet de la Chambre des députés italienne, Paris, 28 septembre 2015.

263 Rapport préc., A/HRC/23/40, pp. 7 et 8.

264 Rapport préc., A/HRC/29/32, p. 7.

265 *Ibid.*, pp. 12 et 13 et §§ 57-60 (recommandations à l'attention des États).

266 Outre la conclusion d'un nouvel accord avec les États-Unis au sujet des données de citoyens européens transférées aux États-Unis, l'affaire *Snowden* a influencé le contenu du RGPD ainsi que la proposition de révision de la directive « *e-privacy* ».

267 En réaction au *LuxLeaks*, la directive 2011/16/UE du 15 février 2011 relative à la coopération administrative dans le domaine fiscal a été modifiée de façon à étendre l'échange automatique de renseignements aux « informations sur les décisions fiscales anticipées en matière transfrontière et les accords préalables en matière de prix de transfert » (art. 8*bis* de la directive 2011/16/UE tel qu'inséré par la directive (UE) 2015/2376 du Conseil du 8 décembre 2015 modifiant la directive 2011/16/UE en ce qui concerne l'échange automatique et obligatoire d'informations dans le domaine fiscal, *J.O.U.E.*, L 332/1 à L 332/10, 18 décembre 2015).

européennes de protection des données, offre une protection certaine au lanceur d'alerte, il ne permet pas de le protéger dans sa globalité. Tandis que la protection qui découle du droit à la liberté d'expression – protection du lanceur d'alerte et protection des sources – se cantonne au signalement public[268], celle tirée du droit à la vie privée et à la protection des données varie en fonction du destinataire du signalement (s'agit-il d'une autorité judiciaire ou pénale ? d'une entreprise ? d'une administration ?) et/ou de l'outil de signalement choisi (le signalement implique-t-il des communications électroniques ?).

70. Un tel cadre lacunaire n'offre assurément pas la sécurité juridique qu'apporterait une règlementation expresse et globale[269]. La proposition de directive du 23 avril 2018 arrive donc à point. Dans la droite ligne des principes de protection établis par la Cour européenne des droits de l'homme, la proposition établit un régime de protection basé sur le respect de trois conditions[270] : *primo*, le lanceur d'alerte devait avoir des motifs raisonnables de croire que l'information rapportée était vraie au moment du signalement ; *secundo*, l'information rapportée doit relever du champ d'application de la directive[271] ; *tertio*, le lanceur d'alerte doit avoir respecté la procédure échelonnée si celle-ci s'imposait. Ces conditions réunies, le lanceur d'alerte doit être protégé contre toute forme de représailles, directe ou indirecte, liée au signalement effectué en vertu de la directive[272].

Au-delà du régime spécifique de protection des lanceurs d'alerte, la proposition de directive souligne l'importance que revêt le respect des droits fondamentaux en la matière. La liberté d'expression et le droit à la protection des données occupent à cet égard une place centrale. L'exigence de confidentialité est particulièrement mise en avant, mais sans être définie, notamment par rapport à la notion d'anonymat.

268 Sur les principales différences qui caractérisent la protection des lanceurs d'alerte et celle des sources journalistiques, voy. not. Q. VAN ENIS, « Une solide protection des sources journalistiques et des lanceurs d'alerte : une impérieuse nécessité à l'ère dite de la "post-vérité" ? », *op. cit.*, pp. 99 et 100.

269 En faveur d'une intervention législative de la part des instances européennes, voy. not. F. COTON et J.-Fr. HENROTTE, « Le lanceur d'alerte : une personne concernée par le traitement de ses données à caractère personnel, mais également par son avenir professionnel… », *op. cit.*, p. 78 ; A. LACHAPELLE, « Protéger les lanceurs d'alerte, un défi de taille », opinion, 22 décembre 2017, *La libre.be*. Voy. aussi en faveur d'une intervention législative tant au plan européen qu'au plan belge, Q. VAN ENIS, « Une solide protection des sources journalistiques et des lanceurs d'alerte : une impérieuse nécessité à l'ère dite de la "post-vérité" ? », *op. cit.*, p. 152.

270 Proposition de directive du 23 avril 2018, art. 13.

271 Sachant que le lanceur d'alerte doit bénéficier de la protection s'il avait des motifs raisonnables de croire que l'information rapportée tombait sous le coup de la directive (considérant n° 60).

272 Proposition de directive du 23 avril 2018, art. 14 et 15.

De la lecture de l'article 11.2 de la proposition de directive, qui oblige l'autorité compétente à accuser réception du signalement reçu, il apparaît que l'anonymat n'a pas été envisagé par la Commission européenne[273]. À l'ère d'Internet, il est regrettable qu'une telle question n'ait pas été abordée et ce d'autant plus que l'anonymat se pratique bel et bien dans les faits, indépendamment de l'échelon de signalement. Sans doute l'ère numérique doit-elle nous conduire à repenser l'anonymat d'une façon plus positive, loin des travers de la dénonciation pratiquée dans les régimes totalitaires, mais sans en oublier les risques latents. Par ailleurs, on s'étonne qu'aucun chapitre n'ait été dédié à la révélation publique d'informations, alors que tel est le cas du signalement interne et du signalement externe[274]. La proposition a cependant le mérite de mettre en lumière le rôle indispensable de source d'information des journalistes d'investigation joué par les lanceurs d'alerte[275]. La révélation publique d'informations constitue sans nul doute une soupape de sécurité nécessaire dans une société démocratique. De plus, son recours direct peut parfois s'imposer dans des circonstances exceptionnelles. Elle ne peut toutefois s'exercer qu'avec la plus grande prudence. Comme nous l'avons souligné, la révélation publique d'informations met en jeu un délicat équilibre entre, d'une part, la valeur de la transparence et, d'autre part, la valeur du secret. Le recours ultime que représente la révélation publique nécessite, à notre sens, un encadrement rigoureux dès lors qu'elle comporte des risques sérieux en termes de réputation, d'image et de vie privée, mais aussi parfois sur le plan de la sécurité nationale, et qu'elle peut témoigner d'une véritable défaillance de notre système.

273 L'obligation de *feed-back* à l'égard du lanceur d'alerte est par ailleurs difficilement conciliable avec un régime d'anonymat (art. 5.1, d) et 9.1, b) de la proposition de directive du 23 avril 2018).

274 Sur ce sujet, voy. la déclaration de European Federation of Journalists (EFJ), European Broadcasting Union (EBU) and News Media Europe (NME), « Whistleblower Directive : the European Commission Takes "an Important Step" but Improvement on Public Reporting yet to be Made », 23 avril 2018, http://europeanjournalists.org/blog/2018/04/23/whistleblower-directive-the-european-commission-takes-an-important-step-but-improvement-on-public-reporting-yet-to-be-made/ (consulté le 23 avril 2018).

275 Proposition de directive du 23 avril 2018, considérant n° 33.